

# Paolo Mori

---

## Computer Science PhD

### Dati Personali

- Data e luogo di nascita:
- Nazionalità:
- Codice Fiscale:
- Contatti: telefono:

e-mail:

webpage:

### 1. Posizioni Ricoperte

- 1.1. **[2011 - oggi]** Responsabile dell'Unità di Ricerca "Trust Security and Privacy" (precedentemente denominata commessa "Trustworthy and Secure Future Internet") dell'Istituto di Informatica e Telematica del Consiglio Nazionale delle Ricerche (prot. AMMCNT-CNR n. 0009894 del 01/02/2011 e prot. 0005747/2020 del 11/09/2020).
- 1.2. **[2021 - oggi]** Primo ricercatore a Tempo Indeterminato presso l'Istituto di Informatica e Telematica del Consiglio Nazionale delle Ricerche dal 1 gennaio 2021.
- 1.3. **[2010 - 2020]** Ricercatore a Tempo Indeterminato presso l'Istituto di Informatica e Telematica del Consiglio Nazionale delle Ricerche dal 1 febbraio 2010 al 31 dicembre 2020.
- 1.4. **[2006 - 2010]** Ricercatore a Tempo Determinato presso l'Istituto di Informatica e Telematica del Consiglio Nazionale delle Ricerche dal 10 maggio 2006 al 31 gennaio 2010.
- 1.5. **[2003 - 2006]** Assegno di Ricerca dell'Istituto di Informatica e Telematica del Consiglio Nazionale delle Ricerche sul tema "Metodologie per una gestione efficiente, affidabile e sicura di computazioni distribuite tramite web services".
- 1.6. **[1999 - 2003]** Dottorato di Ricerca in Informatica conseguito presso il Dipartimento di Informatica dell'Università di Pisa con la tesi "Solving Irregular Problems on Parallel Architecture: a Methodology and a Supporting Library".
- 1.7. **[1998]** Borsa di studio del Consorzio Pisa Ricerche sul tema "Tecnologie dell'informazione, delle comunicazioni e dell'elettronica: sistemi paralleli e software di base".

### 2. Formazione

- Dottorato di Ricerca in Informatica, conseguito presso l'Università degli Studi di Pisa in data 16/12/2003. Titolo della tesi: "Solving Irregular Problems on Parallel Architecture: a Methodology and a Supporting Library".
- Laurea Specialistica in Tecnologie Informatiche, conseguita per abbreviazione di carriera presso l'Università degli Studi di Pisa in data 12/12/2003, con votazione

- Laurea in Scienze dell'Informazione, piano di studi di indirizzo Tecnico, conseguita presso l'Università degli Studi di Pisa in data 24/04/1998, con votazione . Titolo della tesi: "Algoritmi Gerarchici Approssimati su Architetture Parallele a Memoria Distribuita".
- Diploma di Ragioniere Programmatore e Perito Commerciale, conseguito presso l'I.T.C. "A. Einstein" di Firenze nell'anno 1990, con votazione .
- **Esperienze Formative Post Laurea**
  - 4<sup>th</sup> International School on Foundations of Security Analysis and Design, Berlino, 6-11 settembre 2004
  - 2<sup>nd</sup> International Summer School on Grid Computing 2004, Equense, 18-30 luglio 2004
  - 11<sup>a</sup> Scuola Estiva di Calcolo Parallelo; Consorzio Interuniversitario per il Calcolo Automatico dell'Italia Nord Orientale (CINECA), Bologna, settembre 2002
  - 12<sup>th</sup> International School for Computer Science Research "E-Commerce and On-Line Algorithms"; Università di Catania, Lipari, 1-14 luglio 2000
  - 11<sup>th</sup> International School for Computer Science Research "Computational Biology"; Università di Catania, Lipari, 20 giugno - 3 luglio 1999

### 3. **Abilitazione Scientifica Nazionale**

- Settore Concorsuale 01/B1 - INFORMATICA - II Fascia, Dal 07/08/2018 al 07/08/2029

### 4. **Lingue Straniere**

- Ottima conoscenza dell'inglese parlato e scritto, CEF Level C1 - Effective Operational Proficiency, certificato rilasciato da International House Pisa.

### 5. **Gruppi di Lavoro CNR**

- 5.1. Membro del Gruppo di Lavoro per la definizione delle linee guida e della politica dell'Istituto di Informatica e Telematica per il reclutamento del personale per le posizioni a termine (Provvedimento organizzativo 7/2020 prot.n. 0004259/2020 del 02/07/2020);
- 5.2. Membro del gruppo di lavoro IIT per lo svolgimento delle attività nel ambito del progetto "Infrastruttura del Fascicolo Sanitario Elettronico" (provvedimento Organizzativo n. 2 del 15/03/2010 - prot. IIT - CNR - IIT N. 0001694 del 16/03/2010).

### 6. **Altri Gruppi di Lavoro**

- 6.1. Membro Core del Gruppo di Lavoro "Italian Distributed Ledger Technology Working Group, CINI working group on Blockchain" da novembre 2018 (<http://dltgroup.dmi.unipg.it/people.php>);
- 6.2. Membro del Gruppo di Lavoro "Cybersecurity Industry 4.0 Regional Competence Network" della Regione Toscana da luglio 2017;
- 6.3. Membro del Gruppo di Lavoro ERCIM sulla tecnologia Blockchain dal febbraio 2018 (<https://wiki.ercim.eu/wg/BlockchainTechnology/>);
- 6.4. Membro del Gruppo di Lavoro "ECSO-WG6 SRIA: Technical areas, Products, Services areas" di European Cyber Security Organization (ECSO) da settembre 2016;
- 6.5. Membro del gruppo di lavoro "Cloud e Pubblica Amministrazione" di DigitPA (2011-2012), che ha prodotto il documento "Raccomandazioni e proposte sull'utilizzo del Cloud Computing nella Pubblica Amministrazione";

### 7. **Incarichi CNR**

- 7.7. Responsabile dell'Unità di Ricerca "Trust Security and Privacy "(precedentemente denominata commessa "Trustworthy and Secure Future Internet") dell'Istituto di Informatica e Telematica del Consiglio Nazionale delle Ricerche dal febbraio 2011 (AMMONT-CNR n. 0009894 del 01/02/2011 e prot. 0005747/2020 del 11/09/2020).
- 7.6. Membro della struttura di coordinamento dell'Area Progettuale "Cyber Security" del

- Dipartimento Ingegneria, ICT e Tecnologie per l'Energia e i Trasporti (DIITET) del CNR.  
Referente del Tema "Cloud Security" (dal 12/04/2018 con provvedimento 20/2018, prot CNR 0050201/2018 del 17/07/2018)
- 7.5. Membro del Comitato di valutazione per le posizioni a termine dell'Istituto di Informatica e Telematica (Provvedimento Organizzativo 20/2021 - protn. 0004272/2021 del 23/06/2021)
- 7.4. Rappresentante delegato del CNR per i rapporti con EIT Digital
- Rappresentante delegato del CNR al Node Strategic Committee (NSC) dell'Associazione EIT ICT Labs Italy, Co-Location Centre di Trento dal novembre 2016. Partecipato alle riunioni del NSC del 09/07/2019 (prot 0049974/2019 del 09/07/2019) 24/05/2018 (prot 0035547/2018 del 21/05/2018), 18/12/2017 (prot 0082631/2017 del 15/12/2017), 18/05/2017 (prot 0033255/2017 del 16/05/2017), 28/03/2017 (prot CNR IIT n. 0002462 del 21/03/2017), 15/12/2016 (prot AMMCNT-CNR n. 0083442), 13/09/2016 (prot. AMMCNT-CNR n. 0059620).
  - Rappresentante delegato del CNR al Node Strategic Committee (NSC) della Fondazione EIT Digital Italy dal febbraio 2017 (verbale Consiglio di Istituto IIT del 10/01/2017).
  - Rappresentante delegato (Proxy) del CNR alla General Assembly di EIT Digital IVZW del 12/09/2018 (prot CNR-IIT U0009185 del 07/09/2018)
  - Rappresentante delegato (Proxy) del CNR alla General Assembly di EIT Digital IVZW del 08/09/2020 (prot IIT 0005510/2020 del 01/09/2020)
  - Rappresentante delegato (Proxy) del CNR alla General Assembly di EIT Digital IVZW del 15/03/2021 (prot IIT 0001735/2021 del 09/03/2021)
- 7.3. Valutatore del Panel "Tecnologie dell'Informazione e della Comunicazione (TIC)" per il Ministero dello Sviluppo Economico, adesso Ministero delle Imprese e del Made in Italy (lettera di incarico del 15/12/2014, prot AMMCNT-CNR n. 0090103 del 15/12/2014)
- Valutatore progetti per il Ministero dello Sviluppo Economico, Fondo Crescita Sostenibile, Bando Horizon 2020 (Lettera di Incarico prot: AMMCNT-CNR n. 0090103 del 05/12/2014, prot IIT 0005445/2020 del 27/08/2020, prot IIT 0005446/2020 del 27/08/2020)
    - Certified Customer Service Feedback, valutatore primario (Lettera di incarico prot. IIT 0005447/2020 del 27/08/2020)
    - B-Safe Be aware of Cloud Security, valutatore primario (Lettera di incarico prot. 0005448/2020 del 27/08/2020)
    - Smart@Pay: piattaforma abilitante per la gestione di servizi di pagamento su infrastrutture di Smart City, valutatore secondario (Lettera di incarico prot. 0005449/2020 del 27/08/2020)
  - Valutatore progetti per il Ministero dello Sviluppo Economico, Fondo Crescita Sostenibile, Grandi Progetti PON - Agenzia Digitale (Lettera di Incarico del 20/04/2017, prot. IIT 0005450/2020 del 27/08/2020)
    - Semantic Mobility Analyzer (SAMOA) (valutatore unico)
  - Valutatore progetti per il Ministero dello Sviluppo Economico, Fondo Crescita Sostenibile, Horizon 2020 - PON 2014/2020 (lettera di Incarico prot. 00053436/2020 del 01/09/2020)
    - INDAGO: Piattaforma applicativa evoluta per lo screening diagnostico delle patologie cardiovascolari (valutatore unico)
  - Valutatore progetti per il Ministero dello Sviluppo Economico, Fondo Crescita Sostenibile, Sportello Agrifood DM 5/3/2018 (Lettera di Incarico prot IIT: 0005451/2020 del 27/08/2020)
    - ABATA: Applicazioni della Blockchain per l'Autenticazione e la Tracciabilità Alimentare (valutatore unico)
  - Valutatore progetti per il Ministero dello Sviluppo Economico, Fondo Crescita Sostenibile, Sportello Fabbrica Intelligente DM 5/3/2018 (lettera di Incarico prot. 00053434/2020 del 01/09/2020)
    - REASSET: Piattaforma tecnologica MaaS (Maintenance as a Service) basata sull'utilizzo integrato di IoT Blockchain, per la condivisione interoperativa e trasparente di informazioni autenticate e protette, riguardanti la valorizzazione e la gestione operativa in tempo REale degli ASSET tecnico-impiantistici e delle

transazioni tecnico-economiche relative alle interazioni tra i diversi soggetti coinvolti nell'intera filiera del Facility Management (valutatore unico)

- Valutatore progetti per il Ministero dello Sviluppo Economico, Fondo Crescita Sostenibile, Accordo Innovazione Fabbrica Intelligente DM 02/08/2019 (lettera di Incarico prot.CNR 0215857 del 11/07/2023 - UOR: 52)

- Digital-Brand: La trasformazione Digitale dei Brand nel settore fashion e nuove tecnologie emergenti per la gestione del network di produzione e distribuzione (valutatore unico) Valutazione preliminare effettuata a febbraio 2022.

- 7.2. Valutatore di 3 progetti di ricerca congiunta ITALIA - ISRAELE: BANDO PER LA RACCOLTA DI PROGETTI CONGIUNTI DI RICERCA PER L'ANNO 2015, SULLA BASE DELL'ACCORDO DI COOPERAZIONE NEL CAMPO DELLA RICERCA E DELLO SVILUPPO INDUSTRIALE, SCIENTIFICO E TECNOLOGICO TRA ITALIA E ISRAELE ("TRACK INDUSTRIALE"), del Ministero Affari Esteri (MAE) 2015

- 7.1. responsabilità scientifica degli Assegni di Ricerca - Avvisi di Selezione PRIN-2024 PI (bando prot n.0364473 del 04/10/2024 - UOR: 49), 13-2022 (bando prot n. 7897 del 26/10/2022), 04-2021 (bando prot. N. 0002194 del 29/03/2021), 01-2021 (bando prot. IIT N. 0000805 del 02/02/2021), 12-2020 (bando prot IIT N. 0006253 del 30/09/2020), 13-2017 (bando prot. IIT N. 0008993 del 07/11/2017), 16-2016 (bando prot. IIT - IIT N. 0007669 del 21/09/2016), 22-2012 (bando prot. IIT - IIT N. 0005165 del 20/08/2012), 33-2011 (bando prot. IIT - IIT N. 0011147 del 16/12/2011), 13-2011 (bando prot. IIT - IIT N. 0006666 del 14/06/2011),

## 8. Altri Incarichi

- 8.8. Membro della commissione giudicatrice per l'esame finale di conseguimento titolo di dottore di ricerca in "Computer Science and Mathematics", Università Camerino, 2025 (prot. 0053773 del 02/07/2025 - [UOR: SI000086 - Classif VI/6])
- 8.7. Revisore esterno della tesi di dottorato di ricerca in "Information and Communication Technology and Engineering", XXXV ciclo, Università degli Studi di Napoli "Parthenope", del Dr. Fabrizio Marangio intitolata Blockchain for Healthcare Data and Process Management, 2023.
- 8.6. Revisore esterno della tesi di dottorato in Ingegneria Informatica, XXXV ciclo, Università Mediterranea di Reggio Calabria, del Vincenzo De Angelis intitolata Anonymous Protocols for Communications and Service Delivery, 2022.
- 8.5. Membro della commissione giudicatrice del concorso per l'accesso al XXXVII corso di dottorato in informatica, Università di Pisa, nominata con decreto rettoriale del 04/11/2021 del 5 luglio 2021, prot. 77207
- 8.4. Membro del Collegio dei Docenti del dottorato nazionale in intelligenza artificiale nell'area di specializzazione "Sicurezza e Cybersecurity" dell'Università Roma "La Sapienza" per gli anni accademici 2021/2022 e 2022/2023.
- 8.3. Membro supplente della commissione giudicatrice per il concorso di ammissione al XXXVII corso di dottorato in Ingegneria dell'Informazione, tema Tecnologie dell'informazione, Università di Pisa, nominata con decreto rettoriale del 04/11/2021 del 5 luglio 2021, prot. 77207
- 8.2. Membro della commissione giudicatrice del concorso per l'accesso al XXXV corso di dottorato in informatica, Università di Pisa, nominata con decreto rettoriale del 22/11/2019 del 24 aprile 2019
- 8.1. Incarico per la valutazione di N.14 progetti presentati in risposta al bando promosso dal Centro di Competenza START4.0 in tema di tecnologie abilitanti per la sicurezza delle Infrastrutture critiche, aprile 2020 (<https://www.start4-0.it/documenti/start.4.0.bando.progetti.pdf>), lettera incarico PROT. N. 2020/122

## 9. Attività Didattica Universitaria

- 9.11. corso "Mobile and Cloud Security" del Master di I livello in Cyber-Security, Dipartimento di Ingegneria, Università di Pisa

- a.a. 2024/2025 (7 ore), 2025 (Incarico di docenza a titolo oneroso di natura occasionale - Master I livello in "Cybersecurity" presso l'Università di Pisa per l'a.a.2024/2025 Nr. protocollo:Università di Pisa, AOO ICT, 0003500/2025 del 02/09/2025)
  - a.a. 2023/2024 (7 ore), 2024 (Incarico di docenza a titolo oneroso di natura occasionale - Master I livello in "Cybersecurity" presso l'Università di Pisa per l'a.a.2023/2024 Nr. protocollo:Università di Pisa, AOO ICT, 0003223/2024 del 02/09/2024)
  - a.a. 2022/2023 (7 ore), 2023 (Incarico di docenza a titolo oneroso di natura occasionale - Master I livello in "Cybersecurity" presso l'Università di Pisa per l'a.a.2022/223 Nr. protocollo:Università di Pisa, ICT, 0003159/2023 del 03/08/2023)
  - a.a. 2021/2022 (7 ore), 2022 (Incarico di docenza a titolo oneroso di natura occasionale - Master I livello in "Cybersecurity" presso l'Università di Pisa per l'a.a.2021/22, Nr. protocollo:Università di Pisa, ICT, 0003426/2022 del 17/07/2022)
  - a.a. 2020/2021 (8 ore), 2021 (Incarico di docenza a titolo oneroso di natura occasionale - Master I livello in "Cybersecurity" presso l'Università di Pisa per l'a.a.2020/21, Nr. protocollo:Università di Pisa, ICT, 0003850/2021)
  - a.a. 2019/2020 (8 ore), 2020 (Incarico di docenza a titolo oneroso di natura occasionale - Master I livello in "Cybersecurity" presso l'Università di Pisa per l'a.a.2019/20, Nr. protocollo:Università di Pisa, ICT, 0003457/2020 del 25/09/2020)
  - a.a. 2018/2019 (8 ore), 2019 (Incarico di docenza a titolo oneroso di lavoro assimilato - Master I livello in "Cybersecurity" presso l'Università di Pisa per l'a.a.2018/19, Nr. protocollo:Università di Pisa, ICT, 0003566/2019 del 02/08/2019)
  - a.a. 2017/2018 (8 ore), 2018 (Incarico di docenza a titolo oneroso di natura occasionale - Master I livello in "Cybersecurity" presso l'Università di Pisa per l'a.a.2017/18, Nr. protocollo:Università di Pisa, ICT, 0002744/2018 del 26/07/2018)
- 9.10. "Blockchain: applicazioni di cybersecurity" (4 ore) Summer School "Tecnologie digitali per navi sicure", Consiglio Nazionale delle Ricerche e Maritime Technology Cluster FVG S.c.ar.l., edizione 2021
- 9.9. "The Usage Control Model, UCON<sub>ABC</sub>" (1 ora 45 minuti) NeCS PhD Winter School 2018, Università di Trento, 2018
- 9.8. "Enforcing Security Policies on JVM" (2 ore) 6th International School on Foundations of Security Analysis and Design (FOSAD 2006) Martinoro, 2006
- 9.7. Supporto alla didattica per il corso "Laboratorio di Introduzione alla Programmazione I modulo B" del Corso di Laurea in Informatica dell'Università di Pisa 2006/2007 (Delibera n 96/7 del Consiglio di Facoltà nella seduta del 21 settembre 2006)
- 9.6. Supporto alla didattica per il corso "Laboratorio di Programmazione di Rete A" del Corso di Laurea in Informatica dell'Università di Pisa, a.a.2005/2006 (Provvedimento d'urgenza n. del 26/09/2005)
- 9.5. Supporto alla didattica per il corso "Architettura degli Elaboratori B" del Corso di Laurea in Informatica dell'Università di Pisa, 2004/2005 (Provvedimento d'Urgenza n. del 15 ottobre 2004, ratificato dal Consiglio di Facoltà nella seduta del 25 ottobre 2004)
- 9.4. Supporto alla didattica per il corso "Laboratorio di Programmazione di Rete" (18 ore) del Corso di Laurea in Informatica dell'Università di Pisa, a.a.2002/2003, polo didattico di La Spezia
- 9.3. Attività di supporto e assistenza ai docenti per l'elaborazione di contenuti di corsi all'interno del Progetto denominato "Trio" dell'Università di Pisa, 2003
- 9.2. Supporto alla didattica per il corso "Architettura degli Elaboratori I" (20 ore) del Corso di Laurea in Informatica dell'Università di Pisa, a.a.2001/2002 (Delibera 5/2 del Comitato di Presidenza nella seduta del 15 novembre 2001)
- 9.1. Supporto alla didattica per il corso "Informatica Generale" (20 ore) del Corso di Laurea in Scienze Ambientali dell'Università di Pisa 2000/2001
- 10. Altre Docenze**
- 10.8. Docente della lezione "An Introduction to the Blockchain Technology and Bitcoin" nell'ambito del corso "SICUREZZA INFORMATICA" (1 ora), tenutosi al CNR-IIT dal 11 al 13 giugno 2019 (prot IIT n.0006141 del 25/09/2020)
- 10.7. Docente della lezione "Cloud Security" nell'ambito del corso di formazione interno CNR-IIT

- "Corso Cyber Security" (4 ore), tenutosi il 21 settembre 2018 (CNR-IPIT n. U0009905 del 25/09/2018)
- 10.6. Docente del corso di "Programmazione Parallela a Scambio di Messaggi" (36 ore) presso l'Agenzia Spaziale Italiana nell'ambito dell'accordo ASI/CONAE "Strumenti per l'osservazione della terra" nel novembre 2002
- 10.5. Docente del corso di "Architettura e servizi di rete del sistema operativo Windows 2000" (12 ore) presso la società a Lucense (Lucca) nell'ottobre 2001
- 10.4. Docente del corso di "Architettura e servizi di rete del sistema operativo Linux" (50 ore) presso la società a Lucense (Lucca) nell'ottobre 2001
- 10.3. Docente del corso "Networking su Windows NT" (16 ore) presso il centro di formazione "G. Reiss Romoli" di Telecom Italia nel maggio 2001
- 10.2. Docente del corso di alfabetizzazione Windows 2000 ed Office (15 ore) per i dipendenti dell'amministrazione provinciale di Livorno nel febbraio 2001
- 10.1. Docente del corso di "Linux livello avanzato" (40 ore) presso la SSNet (Bologna) nel marzo 2000

## 11. **Supervisore studenti di dottorato, Relatore di Tesi di Laurea, e Tutore di Tirocini**

- 11.23. Co-relatore della tesi di laurea triennale dal titolo "Analisi delle prestazioni della zero-knowledge virtual machine RISC Zero", candidato Gabriele Crisfaro, Dipartimento di Informatica, Università di Pisa, a.a. 2024/2025
- 11.22. Co-relatore della tesi di laurea magistrale dal titolo "Enhancing privacy in SSI with Oblivious Transfer Protocol"; candidato Jacopo Di Domenico, Dipartimento di Ingegneria dell'Informazione, Laurea Magistrale in Cybersecurity, Università di Pisa, a.a. 2023/2024
- 11.21. Tutore del Project Work dal titolo "Integrazione e Strategie per la Cybersecurity nei Sistemi IT Complessi"; candidato Giovanni Quagliato, Dipartimento di Ingegneria dell'Informazione, Università di Pisa, Master I Livello in Cybersecurity, a.a. 2023/2024
- 11.20. Co-relatore della tesi di laurea magistrale dal titolo "Assessing the Trustworthiness of Social Content Through Self-Sovereign Identity"; candidato Calogero Turco, Dipartimento di Informatica, Università di Pisa, a.a. 2023/2024
- 11.19. Co-relatore della tesi di laurea magistrale dal titolo "MERGE: Integrating Self Sovereign Identity in XACML"; candidato Giulio Piva, Dipartimento di Informatica, Università di Pisa, a.a. 2023/2024
- 11.18. Co-relatore della tesi di dottorato dal titolo "Designing Layer-2 Blockchain Applications: Methodologies and Solutions"; candidata Andrea Lisi, Dipartimento di Informatica, Università di Pisa, ciclo XXXVI, 2023.
- 11.17. Supervisore dello studente dottorato Andrea Lisi, Dipartimento di Informatica, Università di Pisa, XXXV ciclo
- 11.16. Supervisore dello studente dottorato Francesco Faloci, Dipartimento di Informatica, Università di Camerino, XXXV ciclo
- 11.15. Correlatore della tesi di laurea triennale dal titolo "NMT: NFT Modificabili per Asset Dinamici nel Metaverso"; candidato Simone Schiavone, Dipartimento di Informatica, Università di Pisa, a.a. 2022/2023
- 11.14. Tutore del Project Work dal titolo "Integrazione di AWS IAM Identity Centre con il servizio OKTA come external IdP"; candidato Claudio Fiorenza, Dipartimento di Ingegneria dell'Informazione, Università di Pisa, Master I Livello in Cybersecurity, a.a. 2021/2022
- 11.13. Co-relatore della tesi di laurea triennale dal titolo "Analisi delle relazioni tra topologia e fee nella Lighting Network di Bitcoin"; candidata Roberta Zucca, Dipartimento di Informatica, Università di Pisa, a.a. 2021/2022
- 11.12. Co-relatore della tesi di laurea triennale dal titolo "Self Sovereign Identity: Analisi e Sviluppo di un Caso d'Uso"; candidato Alessandro Niccolini, Dipartimento di Informatica, Università di Pisa, a.a. 2019/2020
- 11.11. Tutore del Project Work dal titolo "Cloud Security: analisi comparativa delle funzionalità"

- sicurezza messe a disposizione dei servizi Cloud, individuazione di gap e di quali approcci e soluzioni sono stati proposti per colmarli”; candidato: **Andrea Silverstroni**, Dipartimento di Ingegneria dell’Informazione, Università di Pisa, Master I Livello in Cybersecurity, a.a. 2019/2020
- 11.10. Tutore del tirocinio dal titolo “DART: un sistema role-based di reputation e trust management su blockchain Ethereum”; candidato: **Franceschi**, Dipartimento di Informatica, Università di Pisa, a.a. 2019/2020.
- 11.9. Tutore del Project Work dal titolo “Installation and Configuration of Keystone Openstack Cloud Identity Service for Supporting LDAP” candidato: **Presley Kouetolo**, Dipartimento di Ingegneria dell’Informazione, Università di Pisa, Master I Livello in Cybersecurity, a.a. 2018/2019
- 11.8. Tutore del tirocinio dal titolo “Strategia di tokenizzazione di un sistema di recensione su blockchain”; candidato: **Samuel Fabrizi**, Dipartimento di Informatica, Università di Pisa, a.a. 2018/2019.
- 11.7. Supervisore studente dottorato e co-relatore della relativa tesi di dottorato dal titolo: “Privacy-preserving Framework for Decentralized Online Social Networks”; candidato: **De Salve**, Dipartimento di Informatica, Università di Pisa, XXIX ciclo.
- 11.6. Tutore del tirocinio dal titolo “Group-based content sharing: analysis of some encryption techniques”; candidato: **Diego Giorgini**, Dipartimento di Informatica, Università di Pisa, a.a. 2014/2015.
- 11.5. Co-relatore della tesi di laurea dal titolo “Privacy in DOSN: un approccio basato su controllo degli accessi”; candidato: **Filippo Delfino e Alessio Caporale**, Dipartimento di Informatica, Università di Pisa, a.a. 2014/2015.
- 11.4. Tutore del tirocinio dal titolo “Studio e Realizzazione di Meccanismi di Sicurezza in Ambito Grid”; candidato: **Mauro Zampetti**, Facoltà di Ingegneria, Dipartimento di Ingegneria Informatica, Università di Pisa, a.a. 2006/2007.
- 11.3. Tutore del tirocinio dal titolo “Sicurezza nel Grid Computing”; candidato: **Natasha Lasorella**, Facoltà di Ingegneria, Dipartimento di Ingegneria Informatica, Università di Pisa, a.a. 2004/2005.
- 11.2. Co-relatore della tesi di laurea dal titolo “Radioesity Gerarchica in Flatland” studio e Implementazione Parallela mediante la libreria P.I.T.”; candidato: **Matteo Gazzarri**, Dipartimento di Informatica, Università di Pisa, a.a. 2002/2003.
- 11.1. Co-relatore della tesi di laurea dal titolo “Metodologie per la Parallelizzazione di Metodi Multigriglia Adattivi”; candidato: **Sarah Chiti**, Dipartimento di Informatica, Università di Pisa, a.a. 1999/2000.

## 12. Ruoli di Responsabilità in Progetti Europei

- 12.15. **MEDIATE**: Multi faceted Implementation of a mixed software/hardware-based zero-trust framework for the computing continuum. Unfunded HORIZON-CL3-2023-CS-01 project, Grant Agreement 101168465. Ruolo: Coordinatore scientifico per il CNR. Il ruolo nel progetto risulta dalla dichiarazione CNR n. 382569 del 08/10/2025 - UOR: 73. Il progetto si propone di sviluppare una solida tecnologia basata sul modello Fiducia Zero (zero trust) utilizzando strumenti basati sull’intelligenza artificiale per affrontare problemi di sicurezza e privacy nel cosiddetto continuum informatico. Il progetto definisce un controllo basato sulla sicurezza a tutti i livelli del continuum mediante l’impiego di modelli che possono essere aggiornati, ridistribuiti e riconfigurati al suo interno. In questo modo, il progetto consente la resilienza della sicurezza informatica, l’attenuazione delle vulnerabilità e un aumento della fiducia e della sicurezza.
- 12.14. **DLT-Fruit**: A user-centered framework for facilitating DLTs FRUIT. Band 0221 PNRR, P2022N2PJA, 2023-2025. Ruolo: Responsabile dell’Unità Operativa CNR. La partecipazione al progetto e il ruolo di responsabile risultano dal modello A del progetto (sezione 11. List of research units (RU)) e dalla lettera d’incarico 02215103 del 29/06/2024 - UOR: 73. Il progetto DLT-Fruit è finalizzato a creare un ambiente user-friendly per fornire un accesso diretto alle principali Distributed Ledgers agli utenti non esperti. Questo obiettivo sarà raggiunto sfruttando risultati all’avanguardia in diversi campi dell’informatica (sistemi distribuiti, teoria dei grafi e visualizzazione dei dati) per ottenere

risultati in linea con gli obiettivi del PNRR, in particolare per quanto riguarda l'empowerment degli utenti nella sfera digitale, i protocolli delle Distributed Ledger correnti si basano sulla capacità degli utenti di leggere i dati sul Ledger stesso, non può essere ipotizzato per un pubblico ampio, a causa della mancanza di risorse o di know-how tecnico. Le applicazioni esistenti per accedere le Distributed Ledger non rappresentano una soluzione a questo problema, poiché sono componenti di terze parti che reintroducono la necessità della fiducia dell'utente. A questo scopo, il progetto propone un nuovo ambiente che consente agli utenti di accedere ai dati delle Distributed Ledger in modo grafico affidabile, facile da usare e di facile comprensione. Il set di strumenti sarà flessibile e sufficientemente potente da poter essere utilizzato da ricercatori, applicazioni decentralizzate e dal grande pubblico. Tra i suoi contributi teorici, il set di strumenti introdurrà una rappresentazione uniforme per i dati transazionali provenienti da Distributed Ledger eterogenee e fornirà strumenti avanzati di analisi e visualizzazione di grafici temporali all'avanguardia.

- 12.13. **DUCA**: Data Usage Control for empowering digital sovereignty for All citizens. EU funded HORIZON-TMA-MSCA-SE project, Grant Agreement n. 101086308, 2023-2026. Ruolo: Work Package 3 leader. La partecipazione al progetto risulta da PART B1, sezione 4 Participating organisations, Table 7 - Organisations data, Beneficiario: CONSIGLIO NAZIONALE DELLE RICERCHE (CNR). La responsabilità del Work Package 3 risulta dalla dichiarazione di responsabilità prot. 0400313 del 14/12/2023 - UOR: SI00002. L'Internet of Everything ha portato a una forte crescita dei dispositivi connessi, con conseguente generazione di un'enorme quantità di dati. Con il sostegno del programma Marie Skłodowska Curie Actions, il progetto DUCA mira a fornire un framework completo per affrontare le minacce relative alla privacy e alla protezione dei dati. L'obiettivo è consentire ai cittadini e alle organizzazioni europee di assumere il controllo dei propri dati, garantendone la riservatezza e la protezione. Il framework DUCA comprende una serie di soluzioni per la sicurezza e la privacy dei dati, che saranno indipendenti dalla piattaforma per consentire la compatibilità con varie architetture e modelli di implementazione. Il progetto ha identificato tre casi d'uso: energia intelligente, controllo dell'utilizzo di Big Data e intelligenza artificiale, e mobilità collaborativa.
- 12.12. **STRIDE**: Secure and TRaceable Identities in Distributed Environment. progetto dello Spoke 5 del Programma di Ricerca e Innovazione PE00000014, "SEcurity and Rights in the CyberSpace (SERICS)", nell'ambito del Piano Nazionale di Ripresa e Resilienza, finanziato dall'Unione Europea - NextGenerationEU. Ruolo: coordinatore delle attività del CNR dello Spoke 5, Provvedimento Organizzativo n. 0/2023, prot.n. 0053976 del 23/02/2023, lettera di incarico prot.n. 175558 del 08/06/2023. Il progetto è focalizzato sull'identificazione di entità e azioni nel significato generale dei termini, spaziando quindi dagli oggetti agli umani, attraverso domini fisici e virtuali. In questo scenario sono coinvolti molti meccanismi, tecnologie e servizi di sicurezza, a seconda della natura dell'ambiente distribuito, del tipo di entità, dei domini in cui vengono eseguite le interazioni (dal mondo fisico agli ambienti virtuali) e degli obiettivi prefissati (grado di verificabilità, capacità di associazione sicura con altri attributi, tracciabilità, grado di anonimato, ecc.). Per quanto riguarda i meccanismi, il progetto si concentra sui meccanismi crittografici, con un'attenzione specifica verso la crittografia post-quantistica. Per quanto riguarda le tecnologie, STRIDE si concentra sulle tecnologie Distributed Ledger (DLT), blockchain e smart contracts. Per quanto riguarda i servizi, saranno presi in considerazione i cambiamenti evolutivi e le sfide per un'identità digitale sicura e tracciabile come l'identità minima, la protezione dell'identità in ambienti distribuiti, la Self-Sovereign Identity (SSI), e la tracciabilità dei processi.
- 12.11. **DISE**: Digital Sovereignty. progetto dello Spoke 1 del Programma di Ricerca e Innovazione PE00000014, "SEcurity and Rights in the CyberSpace (SERICS)", nell'ambito del Piano Nazionale di Ripresa e Resilienza, finanziato dall'Unione Europea - NextGenerationEU. Ruolo: Work Package 2 Leader. La partecipazione al progetto risulta dalla lettera di incarico prot. n. 175558 del 08/06/2023. La responsabilità del Work Package 2 risulta dalla dichiarazione prot. 0227284 del 01/07/2024 - UOT: 13. Il progetto studia metodi innovativi, basati su Intelligenza Artificiale, per estrarre conoscenze e regole e poi tradurle in politiche di utilizzo dei dati delle risorse computazionali e quindi verificarle e valutarne la conformità con regole interne aziendali, leggi, norme sociali, privacy e/o altri aspetti umani, sociali e legali (Human, Social, and Legal, HSL). Il progetto definisce meccanismi per il controllo dell'utilizzo dei dati e delle risorse computazionali per scenari distribuiti come, ad esempio, l'Internet of Things, i Big Data, il Cloud. Vengono studiati anche gli aspetti

economici, come la comprensione dei costi e degli incentivi per la condivisione dei dati e del valore della sovranità dei dati e delle interazioni. Infine, il progetto studia anche la sovranità dei dati e i modelli di fiducia fornendo approcci di condivisione dei dati adeguati e politiche di controllo dell'utilizzo corrispondenti.

- 12.10. **Tuscany X.0**: Tuscany EU Digital Innovation Hub EU funded H2020 project, Project ID n. 101083396, 2022-2025. Titolo: Task 2.3 leader "Test Before Invest services in Cybersecurity" Tuscany X.0 (TX0) è una federazione che include tutti i principali attori della regione Toscana della ricerca e del trasferimento tecnologico. È composto da 3 System integrator, 3 Access Point e 13 Providers. Tuscany X.0 punta a diventare un System Integrator No-Profit in grado di coordinare l'ecosistema del trasferimento tecnologico per supportare la crescita sostenibile dell'economia della regione Toscana, parallelamente alla valorizzazione dei suoi enti pubblici, e di concorrere con gli altri EDIH all'indipendenza tecnologica dell'Europa. Il progetto promuove l'adozione di tecnologie avanzate nell'ambito del calcolo ad alte prestazioni, dell'intelligenza artificiale e della cybersecurity, attraverso la loro personalizzazione orientata al soddisfacimento delle reali esigenze, requisiti e vincoli industriali.
- 12.9. **SIFIS-Home**: Secure Interoperable Full-Stack Internet of Things for Smart Home: funded H2020 project, Grant Agreement n. 852652, 2020-2023. Titolo: Work Package 4 leader. Costo complessivo del progetto 4 754 875 euro. Costo complessivo CNR per il progetto 600 812,50 euro. La partecipazione al progetto risulta dall'ANNEX 1 (sezione 4 Members of the consortium, sottosezione Participants (Applicants), sottosezione 4.2.1. Consiglio Nazionale delle Ricerche (CNR), Italy), e dalla lettera d'incarico n. 0008454 del 22/12/2022. La responsabilità del Work Package 4 risulta dalla dichiarazione di responsabilità a prot. 207691 del 04/07/2023. Il progetto ha lo scopo di progettare e sviluppare un framework software mirato ad aumentare la sicurezza e la resilienza dei sistemi Smart Home interconnessi, agendo a tutti i livelli dello stack, dal livello kernel/network al livello utente. A tal fine, fornendo opportune librerie per l'interazione con l'ambiente Smart Home, il framework consente a terze parti lo sviluppo di nuove applicazioni e servizi sicuri e privacy-aware, che verranno classificati a seconda del livello di sicurezza e privacy offerto. Inoltre, il framework integrerà un insieme di servizi di base che consentiranno di rilevare tempestivamente e di reagire dinamicamente agli attacchi informatici, ai tentativi di intrusione, e alle violazioni della politica di sicurezza definita dall'Operatore. Questi servizi saranno basati su Intelligenza Artificiale e Deep Learning, per prevenire attacchi alla rete come DoS, side-channel attacks, hijacking, phishing, replay attacks.
- 12.8. **E-CORRIDOR**: Edge enabled Privacy and Security Platform for Multi Modal Transport: EU funded H2020 project, Grant Agreement n. 883135, 2020-2023. Titolo: Work Package 6 leader. Costo complessivo del progetto 5 859 201,25 euro, Contributo EU 4 999 858,38 euro. Contributo complessivo CNR per il progetto 651 250 euro. La partecipazione al progetto risulta dal GRANT AGREEMENT NUMBER 883135 — E-CORRIDOR, ANNEX 1 - Innovation action NUMBER — 883135 — E-CORRIDOR, part B (sezione 4 Members of the consortium, sottosezione Participants (Applicants), sottosezione 4.2.1 Consiglio Nazionale delle Ricerche (CNR), Italy, sottosezione 4.2.1 Key personnel). La responsabilità del Work Package 6 risulta dalla dichiarazione di responsabilità n. 0005490 del 31/08/2020. Il progetto E-CORRIDOR ha lo scopo di progettare e sviluppare un framework flessibile, sicuro e privacy-aware per garantire la sicurezza e la protezione dei sistemi di trasporto multimodale. Infatti, il trasporto collettivo multimodale, ovvero l'impiego di diversi mezzi di trasporto in un singolo percorso di viaggio offre migliori risultati in termini di convenienza, velocità, affidabilità e prevedibilità. Tuttavia, dinanzi alla continua ascesa delle minacce avanzate dagli attacchi informatici, i sistemi di trasporto intelligenti devono essere resi più sicuri. In particolare, il progetto svilupperà un framework per la sicurezza dei passeggeri e degli operatori dei trasporti basato su un sistema di condivisione delle informazioni prodotte da questi ultimi in grado di preservare le loro preferenze di privacy, e sull'esecuzione di analisi collaborative sulle informazioni condivise.
- 12.7. **SPARTA**: Strategic Programs for Advanced Research and Technology in Europe: EU funded H2020 project, Grant Agreement n. 830892, 2019-2023. Titolo: Task 4.4 leader. Costo complessivo del progetto 15.999.913 euro. Costo complessivo CNR per il progetto 720.255 euro. La partecipazione al progetto risulta dall'ANNEX 1 Research and Innovation action NUMBER — 830892 — SPARTA, part B (sottosezione Members of the consortium/Participants (applicants)/Partner 20 Consiglio Nazionale Della Ricerche

(CNR) – Italy/Curriculum Vitae of the primarily responsible person(s) undertaking the work), e dalla lettera d’incarico del 30/01/2019. **PARITA** è una rete di competenze sulla Cybersecurity che mira a creare azioni collaborative di ricerca e innovazione di alto livello. Quattro programmi di ricerca e innovazione forniranno soluzioni avanzate per affrontare le sfide emergenti: bisogni umani di base (salute), attività economiche (energia, finanza e trasporti), tecnologie (ICT e industria) e sovranità (governo elettronico, pubblica amministrazione). Il CNR è Partnership director e contribuisce sia alle attività di costruzione della comunità che a quelle di ricerca. In questo progetto mi occupo della definizione dei requisiti di sicurezza e privacy dei dati mirati alla definizione di un modello comune dei dati e alla scelta della piattaforma di data sharing che deve essere utilizzata nei casi d’uso definiti dal progetto.

- 12.6. **HC & IoT - Privacy Management of Automated Data Generation for Public, Private, and Hybrid Cloud for IoT** : funded by EIT Digital, 2019. Ruolo: Catalyst A1903 leader. EIT funding per il progetto 433.497 euro. Contributo complessivo CNR per il progetto 96.000 euro. La partecipazione al progetto e la responsabilità del Catalyst A1903 risulta dalla Activity Proposal n.19250 della Call 2019 di EIT Digital, e dalla lettera d’incarico del 27 dicembre 2018. Il protocollo IIT 0005458/2020 del 27/08/2020. Il progetto riguarda la progettazione e lo sviluppo di una piattaforma software volta alla protezione dei dati prodotti dai sistemi Internet of Things (IoT) che vengono memorizzati su piattaforme Cloud ibride. Lo scopo del progetto è quello di fornire un framework completo e sicuro per la gestione dei dati rilevati dai sensori IoT, con particolare attenzione agli Big Data, ovvero gli scenari in cui i dispositivi IoT producono enormi quantità di dati che devono essere protetti in quanto memorizzati in Cloud. In questo progetto mi occupo dello studio e progettazione del supporto per la protezione dei dati con particolare attenzione ai problemi derivanti dall’esecuzione del framework in scenari in cui è necessario proteggere enormi quantità di dati.
- 12.5. **Private Virtual Network Federator** funded by EIT Digital, 2018. Ruolo: Catalyst A1805 leader. EIT funding per il progetto 804.356 euro. Contributo complessivo CNR per il progetto 272.813 euro. La partecipazione al progetto e la responsabilità del Catalyst A1805 risulta dalla Activity Proposal n.18167 della Call 2018 di EIT Digital e dalla lettera d’incarico del 27 dicembre 2017. Il progetto riguarda la progettazione e lo sviluppo di una piattaforma per proteggere i sistemi Internet of Things (IoT) di vario tipo, dalla smart home alle smart cities includendo anche gli smart vehicle. Lo scopo del progetto è quello di fornire un framework completo e sicuro per la gestione dei dati rilevati dai sensori IoT, dalla loro rilevazione, alla condivisione e utilizzo, seguendo l’approccio NAC (Network Access Control). Le politiche di sicurezza definite dal progetto, oltre a regolare l’utilizzo dei dati raccolti, sono anche in grado di reagire anche agli eventi rilevati a causa del monitoraggio dei sensori e al comportamento dei dispositivi, in modo da proteggere la rete in modo dinamico. In questo progetto mi occupo dello studio e progettazione del supporto per la protezione dei dati generati dai dispositivi IoT e memorizzati sul Cloud, con particolare attenzione ai problemi derivanti dall’esecuzione del framework per l’enforcement delle politiche di sicurezza sui device IoT, che sono tipicamente poco potenti.
- 12.4. **High Impact Initiative: 14605 Trusted Data Management with Service Ecosystem** funded by EIT Digital, 2017. Ruolo: Catalyst A1726 leader. EIT funding per il progetto 2.300.784 euro. Contributo complessivo CNR per il progetto 130.000 euro. La partecipazione al progetto e la responsabilità del Catalyst A1726 risulta dalla Activity Proposal n.17005 della Call 2017 di EIT Digital, e dalla lettera d’incarico del 22 dicembre 2016. Questo progetto è la continuazione del progetto omonimo del 2016. Nel 2016, 2017 continuo ad occuparmi del sistema per garantire la privacy dei dati multi-soggetto che vengono memorizzati nella piattaforma MY DATA STORE di TIM. In particolare, in quest’anno è stata finalizzata l’integrazione nella piattaforma MY DATA STORE e sono state applicate le ottimizzazioni derivanti dallo studio dei pattern di utilizzo del sistema per migliorare le performance. Inoltre, continuo la progettazione del servizio di usage control per espandere le funzionalità di sicurezza offerte dai servizi di storage forniti da British Telecom. Nel 2017 l’attività si concentra sull’integrazione del nuovo servizio nella piattaforma di storage fornita da British Telecom.
- 12.3. **Collaborative and Confidential Information Sharing and Analysis for Cyber Protection (C3ISP)** : EU funded H2020 project, Grant Agreement n.700294, 2016-2019. Ruolo: Work Package 8 leader. Costo complessivo del progetto 5.000.045,62 euro. Contributo complessivo CNR per il progetto 603.463 euro. La partecipazione al progetto risulta

dall'AMENDMENT Reference No AMD-700294-3 del Grant Agreement 700294 (sottosezione "Key Personnel" della sezione "Partner information" Consiglio Nazionale delle Ricerche (CNR), Italy"), dalla lettera di incarico del 29/10/2016. Da 6 responsabilità del Work Packag 8 risulta dalla dichiarazione di responsabilità a p.0005489 del 31/08/2020. progetto C3ISP ha lo scopo di definire una piattaforma per la condivisione e l'analisi collaborativa delle informazioni fornite da un insieme di (enti, organizzazioni, enti pubblici, etc.) per rilevamento di minacce informatiche e condivisione delle informazioni proposta da C3ISP `e controllata, ovvero il framework permette al fornitore dei dati di definire opportune politiche di usage control per proteggere la privacy dei dati che condivide e dei risultati che verranno prodotti. In questo progetto mi occupo dello studio e progettazione del supporto per l'applicazione delle politiche di usage control che proteggono la privacy dei dati codivisi. Questo supporto deve essere integrato nell'architettura del framework C3ISP a molteplici livelli, allo scopo di eseguire le operazioni stabilite dalla politica per preservare la privacy dei dati.

12.2. **High Impact Initiative:14605 Trusted Data Management with Service Ecosystem** funded by EIT Digital, 2016. Ruolo:Catalyst A1605 leader. EIT funding per il progetto 4.077.102 euro. Contributo complessivo CNR per il progetto 168.000 euro. partecipazione al progetto e la responsabilità. Catalyst A1605 risulta dalla Activity Proposal n.16009 della Call 2016 di EIT Digital. Questo progetto `e la continuazione del progetto omonimo del 2015. Nel 2016 ho continuato ad occuparmi della progettazione di un sistema per garantire la privacy dei dati multi-soggetto che vengono memorizzati nella piattaforma Cloud sviluppata dal progetto stesso. In particolare, i dati in questione vengono memorizzati nella piattaforma MY DATA STORE fornita da TIM. Inoltre, nell'anno 2016 mi sono anche occupato dello studio e progettazione di un servizio per applicare politiche di controllo dell'utilizzo per espandere le funzionalità a di sicurezza offerte dai servizi di storage forniti da British Telecom.

12.1. **High Impact Initiative:14605 Trusted Data Management with Service Ecosystem** funded by EIT ICT Labs, 2015. Ruolo:Catalyst A1511 leader. EIT funding per il progetto 3.000.000 euro. Contributo complessivo CNR per il progetto 60.000 euro. partecipazione al progetto e la responsabilità. Catalyst A1511 risulta dalla Activity Proposal n.15006 della Call 2015 di EIT ICT Labs. In questo progetto mi sono occupato dello studio e della progettazione di un sistema per garantire la privacy dei dati multi-soggetto che vengono memorizzati nella piattaforma Cloud sviluppata dal progetto stesso. In particolare, i dati in questione vengono memorizzati nella piattaforma MY DATA STORE fornita da TIM.

### 13. Partecipazione a Progetti Europei

13.8. **European Network for Cyber Security (NeCS)** , Marie Skłodowska-Curie Actions (MSCA) Innovative Training Networks (ITN): EU funded H2020 project, Grant Agreement n. 675320, 2016-2020. Costo complessivo CNR per il progetto 1.032.245,28 euro. partecipazione al progetto risulta dall'Annex 1 - "Description of the Action" del Grant Agreement n675320, e dalla Dichiarazione di attività n. IIT: 0005747/2020 del 11/09/2020. Il progetto `e orientato alla formazione e sviluppo di un pool di talenti europei per contribuire a mettere in atto e sostenere la strategia di Cyber-security europea, come evidenziato nell'Agenda digitale della Commissione Europea. Data crescente dipendenza della società a dalle tecnologie informatiche e la corrispondente proliferazione di minacce informatiche, vi `e la necessità di far crescere una nuova generazione di giovani ricercatori addestrati a gestire la natura mutevole della prossime sfide della sicurezza informatica. In questo progetto mi occupo di seguire la formazione di alcuni dei dottorandi assegnati al CNR.

13.7. **Confidential and Compliant Clouds (CoCoCloud)** EU funded Collaborative project FP7-ICT-2013-10 Grant Agreement 610853, 2013-2016. Costo complessivo CNR per il progetto 434.505 euro. partecipazione al progetto risulta dall'Annex I - "Description of Work" del Grant Agreement 610853 (sottosezione "Beneficiaries"/"Italian National Research Council"/"Key Personnel") e dalla Dichiarazione di attività n. IIT: 0005747/2020 del 11/09/2020. In questo progetto mi sono occupato dello studio e progettazione dell'architettura del sistema per l'applicazione dei Data Sharing Agreements (DSA) associati ai dati che vengono condivisi tramite il framework utilizzando dispositivi mobili e fissi. Il sistema per l'applicazione dei DSA colleziona in maniera continua il valore gli attributi necessari alla valutazione dei DSA stessi da molteplici sorgenti. Il framework `e

- modulare e configurabile, e ulteriori fonti di attributi possono essere aggiunte con semplicità
- 13.6. **Network of Excellence on Engineering Secure Future Internet Software Services and Systems (NESSOS)** : EU funded NOE project FP7-ICT-2009-5 Grant Agreement n. 256980, 2010-2014. Costo complessivo CNR per il progetto 681.903 euro. Partecipazione al progetto risulta dall'Annex I - "Description of Work" del Grant Agreement n. 256980 (sottosezione "Partner profile"/"Consiglio Nazionale delle Ricerche (CNR)"/"Key Scientific Staff") e dalla Dichiarazione di attività prot.n. IIT: 0005747/2020 del 11/09/2020. Il progetto ha lo scopo di costituire una comunità di ricerca di lunga durata sull'ingegnerizzazione di servizi e sistemi basati su software sicuro. L'approccio di NESSoS si basa sul principio di includere lo studio dei problemi di sicurezza fin dall'inizio dell'analisi e della progettazione del sistema, contribuendo così a ridurre la quantità di vulnerabilità e consentendo il trattamento sistematico della sicurezza nel processo di progettazione. In questo progetto mi sono occupato della progettazione e della realizzazione dell'ambiente di esecuzione basato su Cloud OpenNebula, denominato Cloud Execution Environment (CEE).
  - 13.5. **Comprehensive Approach to cyber roadMap coordinAtion and develOpment (CAMINO)** : Coordination and support action, FP7-SEC-2013-1, Grant agreement n. 607406, 2014-2016. Costo complessivo CNR per il progetto 56.710 euro. Partecipazione al progetto risulta dall'Annex I - "Description of Work" del Grant Agreement n. 607406 (sottosezione "Individual participants"/"Consiglio Nazionale delle Ricerche"/"Key personnel"). Nel progetto ho contribuito alla definizione di una roadmap realistica per migliorare la resilienza delle infrastrutture ICT al cyber-crimine e cyber-terrorismo.
  - 13.4. **Open Computing Infrastructures for Elastic Services (CONTRAIL)** : EU funded IP project FP7-ICT Grant Agreement n. 257438, 2010-2014. Costo complessivo CNR per il progetto 669.660 euro. Il progetto ha lo scopo di definire un framework per la fornitura di servizi Cloud federati di tipo IaaS (fornitura di macchine virtuali) in maniera sicura. La partecipazione al progetto risulta dalla Dichiarazione di attività prot.n. IIT: 0005747/2020 del 11/09/2020. In questo progetto mi sono occupato della progettazione del supporto di sicurezza del framework. Il supporto è basato sul modello di Usage Control, e il contributo innovativo rispetto allo stato dell'arte è che la politica di sicurezza viene verificata non solo al momento della creazione delle macchine virtuali, ma durante l'intera vita del sistema. In caso che una politica di sicurezza venga violata quando una macchina virtuale è in esecuzione, quest'ultima viene interrotta (o sospesa), e vengono eseguite delle azioni definite dalla politica per mitigare gli effetti della violazione.
  - 13.3. **Runtime monitoring for Next Generation Java Platform** : Co-operation project with DoCoMo Euro-Labs, finanziato da DoCoMo Euro-Labs, 2008-2009. Costo complessivo CNR per il progetto 120.811 euro. Partecipazione al progetto risulta dalla Dichiarazione di attività prot.n. IIT: 0005747/2020 del 11/09/2020. Questo progetto mi sono occupato della raffinamento del framework e del prototipo per l'applicazione di politiche di sicurezza basate sul comportamento per applicazioni Java ME (MIDlets) eseguite su telefoni cellulari.
  - 13.2. **Security of Software and Services for Mobile Systems (S3MS)** : EU funded STREP project IST-FP6-027004, Grant Agreement n. 027004, 2006-2008 (www.s3ms.org). Costo complessivo CNR per il progetto 120.811 euro. Partecipazione al progetto risulta dalla Dichiarazione di attività prot.n. IIT: 0005747/2020 del 11/09/2020. Questo progetto ha lo scopo di definire un framework per il deployment e l'esecuzione sicura di applicazioni su dispositivi mobili che comunicano tra loro in ambienti eterogenei. In questo progetto mi sono occupato dello studio e progettazione del componente che implementa l'history-based access control per telefoni cellulari. Il sistema permette di controllare il comportamento delle applicazioni Java Micro Edition (MIDlets) eseguite sul telefono secondo una politica di sicurezza scritta utilizzando il linguaggio CONSPEC. Ho anche sviluppato il prototipo di riferimento per telefoni cellulari con sistema operativo Open Moko.
  - 13.1. **Trust and Security for Next Generation Grids (GridTrust)** : EU funded STREP project IST-FP6-033817, Grant Agreement n. 033817, 2006-2009 (www.gridtrust.org). Costo complessivo CNR per il progetto 228.580 euro. Partecipazione al progetto risulta dalla Dichiarazione di attività prot.n. IIT: 0005747/2020 del 11/09/2020. L'obiettivo del progetto GridTrust è quello di sviluppare la tecnologia per gestire fiducia e sicurezza per i sistemi GRID di prossima generazione. Il progetto propone un approccio verticale ai problemi di fiducia, sicurezza e privacy, partendo dal livello di requisiti fino ai livelli middleware e applicazioni. In questo progetto mi sono occupato della definizione di un modello formale e

dell'architettura del componente per il controllo dell'utilizzo (Usage Control) delle risorse computazionali in sistemi GRID. Ho anche sviluppato il prototipo di riferimento per il controllo di applicazioni Java eseguite in ambienti GRID basati sul framework Globus.

#### 14. Partecipazione a Progetti Nazionali

- 14.7. **Implementazione di Meccanismi per migliorare il consumo Energetico in ambienti Smart Home distribuiti mediante AI e Attribute-based Access Control (IMESHA)**. Ruolo: Responsabile Scientifico e responsabile scientifica del progetto risulta dalla Scheda di Progetto Specifico IMESHA (Allegato B). Nell'ambito dell'automatizzazione delle abitazioni, le cosiddette smart home, il progetto si pone i seguenti obiettivi: 1) studio di tecnologie di Intelligenza Artificiale per la predizione dei profili di consumo energetico; 2) sviluppo di un sistema a regole basato su attributi per prioritizzare il consumo di energia da parte dei dispositivi e valorizzare l'energia prodotta a bassa impronta di carbonio; 3) integrazione nelle case domotiche di dispositivi IoT per il monitoraggio energetico e l'attuazione delle politiche energetiche. Tale sistema dovr`a essere integrato nella soluzione per la smart home prodotta dall'azienda DOMO SRL INNOVATIVA, che partecipa al finanziamento di questo progetto
- 14.6. **Centro di Competenza ad Alta Specializzazione Advances Robotics and Enabling Technologies and System 4.0 (ARTES 4.0)**. Bando MiSE Decreto Ministeriale 214 del 12/09/2017. Importo totale finanziamento 7.499.000 Euro. Ruolo: vice responsabile dell'Awareness Node di Pisa. La partecipazione al progetto e il ruolo di vice-responsabile dell'Awareness Node di Pisa risulta dalla "Proposta per la Costituzione del Centro di Competenza ad Alta Specializzazione Advanced Robotics and enabling digital Technologies & Systems 4.0 - ARTES 4.0", "ALLEGATO C - PROPOSTA TECNICA", sezione 4.1.1.11 "Consiglio Nazionale delle Ricerche (CNR)". La partecipazione al progetto risulta anche dalle lettera di incarico nr protocollo IIT 0003/2020 del 21/05/2020. Centro di Competenza (CC) ARTES 4.0 `e una rete ad alta specializzazione, nell'ambito delle aree della robotica avanzata e delle tecnologie digitali abilitanti collegate, in grado di fornire tecnologie e servizi dedicati a rispondere ai bisogni delle imprese, in particolare le PMI, mediante progetti di orientamento, formazione, innovazione, ricerca industriale e sviluppo sperimentale.
- 14.5. **Operational Knowledge from Insights and Analytics on Industrial Data (OK-INSOID)**: finanziato dal Ministero dell'Istruzione, Universita` e Ricerca (MIUR), Bando PON e FSC - Fabbrica Intelligente. Inizio attivita`: 01/07/2018, termine attivita` 31/01/2021. Budget complessivo: 834.393,00 euro. OK-INSOID propone innovazione scientifica, tecnologica e applicativa grazie all'introduzione delle Big Data Analytics nel contesto industriale, contribuendo a ridisegnare i processi di produzione e i modelli di business, per ottenere, grazie ai dati e alle analitiche, un cambio di passo nella creazione di servizi digitali per il settore industriale. OK-INSOID riconosce il potenziale dei dati provenienti dalle realta` produttive, ancora sottosfruttati, ma le aziende non possiedono sufficienti competenze per estrarre il valore, talvolta nascosto, contenuto al loro interno ("insider") tale ragione, OK-INSOID adottera` avanzate tecnologie allo stato dell'arte, definendo nuove applicazioni industriali data driven. OK-INSOID propone, inoltre, un nuovo approccio alle analitiche, basato sulla coordinazione, collaborazione e sincronizzazione di quelle esistenti a livello cloud e a livello edge. L'approccio sar`a supportato dall'adozione di un'architettura di riferimento e da una sua implementazione, finalizzate allo sviluppo di nuove analitiche ibride "cloud-edge" per l'Industria 4.0.
- 14.4. **Piattaforme Cloud Sicure per applicazioni critiche - caso del Fascicolo Sanitario Elettronico (PiCS)**: progetto POR CRO FSE 2007-2013 Asse IV Capitale Umano finanziato dalla Regione Toscana e da DEDALUS SpA (Responsabile Scientifico). Il finanziamento del progetto risulta dal Decreto N. 2460 del 30 Maggio 2012 della REGIONE TOSCANA, DIREZIONE GENERALE COMPETITIVITA' DEL SISTEMA REGIONALE E SVILUPPO DELLE COMPETENZE, AREA DI COORDINAMENTO RICERCA. La responsabilita` scientifica del progetto risulta dalla Scheda di Progetto Specifico n.8 PiCS, e dalla Dichiarazione di attivita` prot.n. IIT: 0005747/2020 del 11/09/2020. Nell'ambito di questo progetto mi sono occupato della progettazione ed ho contribuito alla implementazione di una soluzione basata su un Cloud open source per l'esecuzione della piattaforma clinico-sanitaria X1.V1 (prodotto commerciale fornito da DEDALUS SpA) a supporto dell'interoperabilita` e della cooperazione fra unita` ospedaliere territoriali. Inoltre, mi

sono occupato di progettare ed ho contribuito a realizzare il supporto di sicurezza avanzato, integrato con la soluzione Cloud definita ed implementata.

- 14.3. **Evoluzione e interoperabilit a tecnologica del Fascicolo Sanitario Elettronico** : finanziato dal Dipartimento per la Digitalizzazione della Pubblica Amministrazione e l'Innovazione Tecnologica della Presidenza del Consiglio dei Ministri, 2010-2013. Questo progetto rappresenta la prosecuzione dei due progetti precedenti, e la partecipazione risulta dal Provvedimento organizzativo del 15/03/2010 dell'Istituto di Informatica e Telematica del Consiglio Nazionale delle Ricerche, prot. CNR - IIT N. 0001694 del 16/03/2010, in cui viene costituito un gruppo di lavoro apposito. Il progetto era finalizzato ad accelerare lo sviluppo di servizi innovativi atti a facilitare la cooperazione e l'interoperabilit  di piattaforme regionali, anche in ambiente Cloud e con tecnologia open source, nonch e attraverso la sperimentazione di nuovi servizi di tele-assistenza per il cittadino.
  - 14.2. **Realizzazione di un'infrastruttura operativa a supporto dell'interoperabilit a delle soluzioni territoriali di Fascicolo Sanitario Elettronico nel contesto del Sistema Pubblico di Connettivit a** finanziato dal Dipartimento per la Digitalizzazione della Pubblica Amministrazione e l'Innovazione e Tecnologie della Presidenza del Consiglio dei Ministri, 2010-2011. Questo progetto rappresenta la prosecuzione del progetto precedente, e la partecipazione risulta dal Provvedimento organizzativo del 15/03/2010 dell'Istituto di Informatica e Telematica del Consiglio Nazionale delle Ricerche, prot. CNR - IIT N. 0001694 del 16/03/2010, in cui viene costituito un gruppo di lavoro apposito.
  - 14.1. **Infrastruttura tecnologica del Fascicolo Sanitario Elettronico** finanziato dal Dipartimento Innovazione e Tecnologie della Presidenza del Consiglio dei Ministri. La partecipazione al progetto risulta dal Provvedimento organizzativo del 15/03/2010 dell'Istituto di Informatica e Telematica del Consiglio Nazionale delle Ricerche, prot. CNR - IIT N. 0001694 del 16/03/2010, in cui viene costituito un gruppo di lavoro apposito.
15. **Trasferimento Tecnologico**
- 15.8. **Socio fondatore e advisor scientifico della societ a DOMO SRLS INNOVATIVA** (P.IVA: 02450970500, C.F.02450970500), costituita in data 13 luglio 2022 (Atto di costituzione registrato a MILANO - Direzione Provinciale 2, il 15 luglio 2022, serie 1T), spin-off del Politecnico di Torino (Delibera del Consiglio di Amministrazione dell'Ateneo del 30 novembre 2022, Prot.0060101 del 14/12/2022) chiesta per diventare spin-off del CNR sottomessa a ottobre 2022 e accettata nel 2023 (Deliberazione del Consiglio di Amministrazione del CNR del 28 aprile 2023, Prot. 000148/2023 - Verb. 476)
  - 15.7. **HC & IoT - Privacy Management of Automated Data Generation for Public, Private, and Hybrid Cloud for IoT** : funded by EIT Digital, 2019 (Catalyst A1903 leader). Aziende partecipanti: British Telecom, Reply, Huawei;
  - 15.6. **Private Virtual Network Federator** funded by EIT Digital, 2018 (Catalyst A1805 leader). Aziende partecipanti: British Telecom, Reply, Huawei;
  - 15.5. **High Impact Initiative:14605 Trusted Data Management with Service Ecosystem** funded by EIT Digital, 2017 (Catalyst A1734 leader). Aziende partecipanti: TIM, British Telecom;
  - 15.4. **High Impact Initiative:14605 Trusted Data Management with Service Ecosystem** funded by EIT Digital, 2016 (Catalyst A1605 leader). Aziende partecipanti: TIM, British Telecom;
  - 15.3. **High Impact Initiative:14605 Trusted Data Management with Service Ecosystem** funded by EIT ICT Labs, 2015 (Catalyst A1511 leader). Aziende partecipanti: TIM, British Telecom;
  - 15.2. **Piattaforme Cloud Sicure per applicazioni critiche: caso del Fascicolo Sanitario Elettronico (PiCS)**: progetto POR CRO FSE 2007-2013 Asse IV Capitale Umano finanziato dalla Regione Toscana e da DEDALUS SpA (Responsabile Scientifico) e partecipanti Dedalus SpA.
  - 15.1. **Runtime monitoring for Next Generation Java Platform** Co-operation project with DoCoMo Euro-Labs, finanziato da DoCoMo Euro-Labs, 2008-2009.
16. **Paper Awards**

- 16.1.D. W Chadwick, W. Fan, G. Constantino, R. De Lemos, F. Di Cerbo, I. Herwonod, P. Mori, A. Sajjad, X. Wang: *A Cloud-Edge based Data Security Architecture for Sharing and Analyzing Cyber Threat Information*. In *Future Generation Computer Systems* Elsevier Science, vol.102, pp.710–722 (2020) DOI 10.1016/j.future.2019.06.026, ISSN 0167-739X, Editor's choice paper for Spring 2022
- 16.2.A. La Marra, F. Martinelli, P. Mori, A. Rizos and A.Saracino: *Using IFTTT to Express and Enforce UCON Obligations*. In *Proceedings of the 15th International Conference on Information Security Practice and Experience (ISPEC2019)*, Lecture Notes in Computer Science 11879, Springer, 213–231, DOI 10.1007/978-3-030-34339-2\_12, ISBN 978-3-030-34339-2, Best Paper Award
- 16.3.H. Koshutanski, F. Martinelli, P. Mori and A. Vaccarelli: *Fine-grained and History-based Access Control with Trust Management for Autonomic Grid Services*. In *Proceedings of International Conference on Autonomic and Autonomous Systems (ICAS06)* IEEE Computer Society (2006) 34, ISBN 0-7695-2653-5, DOI 10.1109/ICAS.2006.25, Best Paper Award

## 17. Pubblicazioni in Riviste Internazionali

- 17.41.: A. De Salve, A. Lisi, M. Cascino, P. Mori and L. Ricci, *Selective Disclosure Approaches in Self-Sovereign Identity: An Experimental Comparison*. in *IEEE Access*, vol.14, pp. 1152-1181, 2026, DOI: 10.1109/ACCESS.2025.3649167
- 17.40.L. Alajramya, M. Simoni, M. Rasori, A. Saracino, P. Mori: *On-Device Derivation of IoT Usage Control Policies: Automating U-XACML Policy Generation from Natural Language with LLMs in Smart Homes Environments*. In *Future Generation Computer Systems*, Volume 175, February 2026, 108067, DOI 10.1016/j.future.2025.108067
- 17.39.M. Rasori, A. Aldini, P. Mori, A. Saracino: *Exploiting Usage Control for Implementation and Enforcement of Security by Contract*. In *Internet of Things*, Volume 33, September 2025, 101697, DOI: 10.1016/j.iot.2025.101697
- 17.38.D. Tortola, A. Lisi, P. Mori, L. Ricci: *Tethering Layer 2 solutions to the blockchain: A survey on proving schemes*. In *Computer Communications*, 2024, Volume 225, pp 289-310, DOI: 10.1016/j.comcom.2024.07.017
- 17.37.W. Abbasi, P. Mori, A. Saracino: *Trading-off Privacy, Utility, and Explainability in Deep Learning-based Image Data Analysis*. In *IEEE Transactions on Dependable and Secure Computing*, 2024, DOI: 10.1109/TDSC.2024.3400608
- 17.36.M. Rasori, A. Saracino, P. Mori, M. Tiloca: *Using the ACE framework to enforce access and usage control with notifications of revoked access rights*. In *International Journal of Information Security*, 2024, DOI: 10.1007/s10207-024-00877-1
- 17.35.A. De Salve, D. Di Francesco Maesa, P. Mori, L. Ricci, A. Puciani: *A multi-layer trust framework for Self Sovereign Identity on blockchain*. In *Online Social Networks and Media*, Volumes 37–38, 2023, pp 100265, DOI: 10.1016/j.osnem.2023.100265, ISSN 2468-6964
- 17.34.S. Bistarelli, Francesco Faloci, Paolo Mori, *A framework for automating the modeling of blockchain based supply chain tracing systems* In *Future Generation Computer Systems*, Volume 149, pp 679-700, 2023, DOI: 10.1016/j.future.2023.07.012, ISSN 0167-739X
- 17.33.A. De Salve, P. Mori, L. Ricci, R. Di Pietro: *Content Privacy Enforcement Models in Decentralized Online Social Networks: State of Play, Solutions, Limitations, and Future Directions*. In *Computer Communications*, Volume 203, pp 199-225, 2023, DOI: 10.1016/j.comcom.2023.02.023
- 17.32.D. Di Francesco Maesa, A. Lisi, P. Mori, L. Ricci, G. Boschi: *Self sovereign and blockchain based access control Supporting attributes privacy with zero knowledge*. In *Journal of Network and Computer Applications*, vol 212, pp 103577, 2023, DOI: 10.1016/j.jnca.2022.103577, ISSN 1084-8045
- 17.31.F. Martinelli, P. Mori, O. Oleksii, A. Saracino: *Cyber Threat Intelligence for Critical Infrastructure Security*. In *Concurrency and Computation in Practice and Experience*, 2023, DOI: 10.1002/cpe.7759
- 17.30.A. De Salve, L. Franceschi, A. Lisi, P. Mori, L. Ricci: *DART: A trust management system integrating blockchain and off-chain computation*. In *ACM Transactions on Internet Technology*, vol.23 issue 1, article no.4 pp 1–30, (2023), available online on 19 September 2022 (2022), DOI 10.1145/3561386, ISSN: 1533-5399, EISSN: 1557-6051

- 17.29.L. Ardito, L. Barbato, P. Mori and A. Saracino *Preserving Privacy in the Globalized Smart Home: The SIFIS-Home Project*. In IEEE Security & Privacy, vol 20 number 1, pp.33-44 (online 2021, printed 2022), DOI: 10.1109/MSEC.2021.3118561, ISSN: 1540-7993
- 17.28.G. Giorgi, A. La Marra, F. Martinelli, P. Mori, A. Rizos, A. Saracino *Exploiting IFTTT and Usage Control Obligations for SmartHome Security and Management*. In Concurrency and Computation: Practice and Experience, e6189 (2022) DOI: 10.1002/cpe.6189, ISSN: 15320626
- 17.27.A. Lisi, A. De Salve, P. Mori, L. Ricci, S. Fabrizio *Rewarding reviews with tokens: An Ethereum-based approach* In Future Generation Computer Systems, Elsevier Science, vol. 120, pp.36-54 (2021), DOI: 10.1016/j.future.2021.02.003, ISSN: 0167739X
- 17.26.A. De Salve, P. Mori, B. Guidi, L. Ricci, R. Di Pietro *Predicting Influential Users in Online Social Networks Groups*. In ACM Transactions on Knowledge Discovery from Data, vol. number 3, pp 35:1-35:50 (2021) DOI: 10.1145/3441447
- 17.25.B. Martini, P. Mori, F. Marino, A. Saracino, A. Lunardelli, A. La Marra, F. Martinelli, P. Castoldi: *Pushing forward Security in Network Slicing by leveraging Continuous Usage Control*. In IEEE Communications Magazine, IEEE, vol. 58 number 7, pp 65-71 (2020), DOI 10.1109/MCOM.001.1900712, ISSN 01636804
- 17.24.G. Baldi, Y. Diaz, T. Dimitrakos, F. Martinelli, C. Michailidou, P. Mori, O. Osliak and Andrea Saracino *Session-dependent Usage Control for Big Data* In Journal of Internet Services and Information Security, vol. no.3, pp.76-92 (August 2020) DOI 10.22667/JISIS.2020.08.31.076, ISSN 21822069
- 17.23.D. W Chadwick, W. Fan, G. Constantino, R. De Lemos, F. Di Cerbo, I. Herwonod, P. Mori, A. Sajjad, X. Wang: *A Cloud-Edge based Data Security Architecture for Sharing and Analyzing Cyber Threat Information*. In Future Generation Computer Systems, Elsevier Science, vol. 102, pp.710-722 (2020) DOI 10.1016/j.future.2019.06.026, ISSN 0167-739X
- 17.22.D. Di Francesco Maesa, P. Mori *Blockchain 3.0 Applications Survey*. In Journal of Parallel and Distributed Computing, vol. 38, pp 99-114 (2020), DOI 10.1016/j.jpdc.2019.12.019, ISSN 07437315
- 17.21.A. De Salve, P. Mori, B. Guidi, L. Ricci *An analysis of the internal organization of Facebook groups*. In IEEE Transactions on Computational Social Systems, vol. 6, pp.1245-1256 (2019), DOI 10.1109/TCSS.2019.2942076, ISSN 2329-924X
- 17.20.D. Di Francesco Maesa, P. Mori, L. Ricci *A blockchain based approach for the definition of auditable Access Control systems*. In Computers & Security, Elsevier Science, vol. 84, pp. 93-119, (2019) DOI 10.1016/j.cose.2019.03.016, ISSN 0167-4048
- 17.19.A. De Salve, B. Guidi, L. Ricci, P. Mori *Discovering Homophily in Online Social Networks*. In Mobile Networks and Applications vol. 23(6), pp.1715-1726, (2018) DOI 10.1007/s11036-018-1067-2, ISSN 1383-469X
- 17.18.A. De Salve, P. Mori, L. Ricci *A Survey on Privacy in Decentralized Online Social Networks*. In Computer Science Review, Elsevier, vol. 27, pp.154-176, (2018) DOI 10.1016/j.cosrev.2018.01.001, ISSN 1574-013
- 17.17.A. Bertolino, A. Calabro', F. Di Giandomenico, G. Lami, F. Lonetti, E. Marchetti, F. Martinelli, I. Matteucci, P. Mori: *A Tour of Secure Software Engineering Solutions for Connected Vehicles*. In Software Quality Journal, Springer vol. 26, issue 4, pp.1223-1256, (2018), DOI 10.1007/s11219-017-9393-3, ISSN 0963-9314
- 17.16.A. De Salve, R. Di Pietro, P. Mori, L. Ricci *A Logical Key Hierarchy Based approach to preserve content privacy in Decentralized Online Social Networks*. In IEEE Transactions on Dependable and Secure Computing vol. 17(1), no.1, pp.2-21, 1 Jan.-Feb 2020, Date of Publication: 20 July 2017, DOI 10.1109/TDSC.2017.2729553, ISSN: 1545-5971 (printed)
- 17.15.A. De Salve, B. Guidi and P. Mori *Predicting the availability of users devices in Decentralized Online Social Networks*. In Concurrency and Computation: Practice and Experience, vol. 30, issue 20, (2018) DOI 10.1002/cpe.4390 ISSN 1532-0626
- 17.14.A. Lazouski, F. Martinelli, P. Mori, A. Saracino *Stateful Data Usage Control for Android Mobile Devices*. In International Journal of Information Security, Springer, Volume 16, Issue 4, pp 345-369, (2017) DOI 10.1007/s10207-016-0336-y, ISSN 1615-5262 (printed), 1615-5270 (online)
- 17.13.E. Carniani, D. D'Arenzo, A. Lazouski, F. Martinelli, P. Mori *Usage Control on Cloud*

- Systems. In Future Generation Computer Systems, Elsevier Science, vol.3(C), pp.37-55, (2016), DOI 10.1016/j.future.2016.04.010, ISSN 0167-739X
- 17.12.E. Carniani, G. Costantino, F. Martinelli, P. Mori, F. Marinelli: *Enhancing Video Surveillance with Usage Control and Privacy-Preserving Solutions*. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), vol.4, pp.20-40, (2016), DOI 10.22667/JOWUA.2016.12.31.020, ISSN 2093-5374
- 17.11.E. Marzini, P. Mori, S. Di Bona, D. Guerri, M. Lettere, L. Ricci: *Tool for Managing the X1.V1 Platform on the Cloud*. In Scalable Computing Practice and Experience, vol.16, issue 1, pp103-120, (2015) DOI 10.12694/scpe.v16i1.1063, ISSN 1895-1767
- 17.10.A. Bertolino, S. Daoudagh, F. Lonetti, E. Marchetti, F. Martinelli, P. Mori: *Testing of PoIPA Authorization Systems*. In Software Quality Journal, Springer, vol.22, issue 2, pp241-271, (2014), DOI 10.1007/s11219-013-9216-0, ISSN 0963-9314 (printed), 1573-1367 (online)
- 17.9.G. Karopoulos, F. Martinelli, P. Mori: *Usage control in SIP-based multimedia delivery*. In Computers & Security, Elsevier Science, vol 39, part 4, pp409-418, (2013) DOI: 10.1016/j.cose.2013.09.005, ISSN 0167-4048
- 17.8.M. Colombo, F. Martinelli, P. Mori, B. Martini, M. Gharbaoui, P. Castoldi: *Extending Resource Access in Multi-Provider Networks using Trust Management*. In International Journal of Computer Networks and Communications (IJCNC) Academy & Industry Research Collaboration Center (AIRCC) (2011), 133-147, ISSN 0974-9322(online), 0975-2293(print), DOI:10.5121/ijcnc.2011.3309
- 17.7.A. Lazouski, F. Martinelli, P. Mori: *Usage control in computer security: A survey*. In Computer Science Review, Elsevier, vol.4, issue 2, pp81-99, (2010) DOI: 10.1016/j.cosrev.2010.02.002, ISSN 1574-0137
- 17.6.F. Martinelli, P. Mori: *On Usage Control for GRID Systems*. In Future Generation Computer Systems, Elsevier Science, vol.16, issue 7, pp1032-1042, (2010) DOI:10.1016/j.future.2009.12.005, ISSN 0167-739X
- 17.5.G. Costa, F. Martinelli, P. Mori, C. Schaefer, T. Walter: *Runtime Monitoring for Next Generation Java ME Platform*. In Computers & Security, Elsevier Science, vol.19, issue 1, pp. 74-87, (2010) DOI: 10.1016/j.cose.2009.07.005, ISSN 0167-4048
- 17.4.M. Colombo, A. Lazouski, F. Martinelli, P. Mori: *Controlling the Usage of Grid Services*. In International Journal of Computational Science 4(3), Special Issue Recent Advance in Computing Technologies, Global Information Publisher (2009), 373-386, ISSN 1992-6669 (print) 1992-6677 (online)
- 17.3.H. Koshutanski, A. Lazouski, F. Martinelli, P. Mori: *Enhancing Grid security by fine-grained behavioral control and negotiation-based authorization*. In International Journal of Information Security, Springer, vol.8, issue 4, pp291-314, (2009) DOI 10.1007/s10207-009-0083-4, ISSN 1615-5262
- 17.2.P. Mori and L. Ricci: *Computational Science in High School: Defining Curricula and Environment*. In Special Issue of Future Generation Computer Systems, "Education in the Computational Science", Elsevier Science, vol.10, issue 8, pp1349-1361, (2003) DOI 10.1016/s0167-739X(03)00092-X, ISSN 0167-739X
- 17.1.F. Baiardi, S. Chiti, P. Mori and L. Ricci: *Integrating Load Balancing and Locality in the Parallelization of Irregular Problems*. In Future Generation Computer Systems, Elsevier Science, vol.17, issue 8, pp969-975, (2001) DOI 10.1016/S0167-739X(01)00039-5, ISSN 0167-739X

## 18. Pubblicazioni in Conferenze e Workshop Internazionali

- 18.115.F. Donini, D. Di Francesco Maesa, P. Mori, L. Ricci: *Tool for the Simulation of Smart Contract Lifecycles Based on Usage Patterns*. In proceedings of the 8th International Conference on Blockchain Technology and Applications (ICBTA 2025)
- 18.114.A. Giuliani, A. De Salve, P. Mori, L. Ricci: *VeriCert: SSL/TLS Certificate Verification based on Self-Sovereign Identity and Blockchain*. In proceedings of the 4th EAI International Conference on Blockchain Technology and Emerging Applications (blockTEA 2025)
- 18.113.C. Turco, A. De Salve, D. Di Francesco Maesa, P. Mori, L. Ricci: *Aid to Mitigate Online Misinformation with Self-Sovereign Identity and Artificial Intelligence*. In proceedings of the

- 7th International Conference on Blockchain Computing and Applications (BCCA 2025), 2025
- 18.112. G. Ciarmella, F. Martinelli, F. Mercaldo, P. Mori, A. Santoro. *Federated Machine Learning Method for Malicious Smart Contract Detection*. In proceedings of the 7th International Conference on Blockchain Computing and Applications (BCCA 2025), 2025
- 18.111. A. Breglia, A. De Salve, P. Mori and L. Ricci. *Assessing the Anonymity of DIDs in Self-Sovereign Identity*. In proceedings of the 7th Distributed Ledger Technology Workshop (DLT 2025), 2025
- 18.110. S. Bistarelli, I. Mercanti, P. Mori and C. Taticchi. *Introducing Event-Driven Properties Management in \*-chain*. In proceedings of the 7th Distributed Ledger Technology Workshop (DLT 2025), 2025
- 18.109. L. Alajramy, P. Mori. *Behavior-Based Anomaly Detection in Access and Usage Control for Smart Home Environments*. In proceedings of the 20th International Conference on Availability, Reliability and Security (ARES 2025), Lecture Notes in Computer Science, vol 15997. Springer, Cham, 2025, DOI: 10.1007/978-3-032-00639-4\_17297-315
- 18.108. Damiano Di Francesco Maesa, Francesco Donini, Paolo Mori, Laura Arsiculazione. *Simulation Engine for Evaluating Smart Contract Based Applications Sustainability*. In proceedings of the 2025 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), 2025, 495-500, IEEE Computer Society
- 18.107. A. De Salve, D. Di Francesco Maesa, P. Mori, G. Piva, L. Ricci. *Integrating Self Sovereign Identity in XACML: the MERGE Approach*. In proceedings of the 32nd International Conference on Enabling Technologies for Infrastructure for Collaborative Enterprises (WETICE 2024)
- 18.106. D. Di Francesco Maesa, F. Donini, P. Mori, L. Ricci. *Protecting Non Fungible Mutable Tokens: an Application in the Metaverse*. In Proceedings of IEEE International Conference on Blockchain and Cryptocurrency (IEEE ICBC 2024)
- 18.105. D. Tortola, A. Pelosi, G. Russo, P. Mori, L. Ricci. *zkSNARK Libraries for Blockchains: a Comparative Study*. In Proceedings of the Sixth Distributed Ledger Technology Workshop (DLT 2024), CEUR Workshop Proceedings (2024)
- 18.104. W. Abbasi, P. Mori and A. Saracino. *Further Insights: Balancing Privacy, Explainability, and Utility in Machine Learning-based Tabular Data Analysis*. In Proceedings of the 19th International Conference on Availability, Reliability and Security (ARES), 2024, 176:1-176:10, DOI: 10.1145/3664476.3670901
- 18.103. S. Bistarelli, F. Faloci, M. Miculan, P. Mori, C. Taticchi. *Modeling Carne PRI supply chain with the \*-Chain Platform*. In Proceedings of the Fifth Distributed Ledger Technology Workshop (DLT 2023), CEUR Workshop Proceedings (2023), Volume 3460
- 18.102. W. Abbasi, P. Mori, A. Saracino. *Privacy-Preserving Object Recognition with Explainability in Smart Systems*. In Proceedings of Private, Secure, and Trustworthy AI 2023 (prist-ai-2023)
- 18.101. W. Abbasi, P. Mori, A. Saracino. *The Explainability-Privacy-Utility Trade-off for Machine Learning-based Tabular Data Analysis*. In Proceedings of 20th International Conference on Security and Cryptography (SECRYPT 2023)
- 18.100. A. De Salve, D. Di Francesco Maesa, F. Federico, P. Mori, L. Ricci. *AlgoID: a blockchain reliant Self-Sovereign Identity framework on Algorand*. In Proceedings of IEEE Symposium on Computers and Communications (IEEE ISCC 2023)
- 18.99. A. Lisi, N. Lopardo, D. Tortola, P. Mori, L. Ricci and F. Severino. *A cross-chain rating system: bridging EVM-based blockchains with Chainbridge*. In Proceedings of IEEE International Conference on Omni-Layer Intelligent Systems (IEEE COINS 2023)
- 18.98. D. Di Francesco Maesa, A. Lisi, P. Mori, L. Ricci, S. Schiavone. *Non Fungible Mutable Tokens: dynamic assets traceability for the Metaverse*. In Proceedings of IEEE International Conference on Metaverse Computing, Networking and Applications (IEEE MetaCom 2023)
- 18.97. A. De Salve, A. Lisi, P. Mori, L. Ricci, C. Turco. *Self-Sovereign Identity for Privacy-Preserving Shipping Verification System*. In Proceedings of the 5th International Conference on Blockchain Technology and Applications (ICBTA 2022), pp 147-157, DOI 10.1145/3581971.3581992

- 18.96. S. Bistarelli, F. Faloci, P. Mori, C. Taticchi. *Olive Oil as Case Study for the \*-Chain Platform*. In proceedings of the 4th Distributed Ledger Technology Workshop (DLT 2022) in conjunction with ITASEC 2022/EUR Workshop Proceedings (2022), volume 3166, pp 94-102
- 18.95. W. Abbasi, P. Mori, A. Saracino, V. Frascolla. *Privacy Vs Accuracy Trade-Off in Privacy Aware Face Recognition in Smart Systems*. In Proceedings of the 12th Workshop on Management of Cloud and Smart City Systems, in conjunction with 2022 IEEE Symposium on Computers and Communications (ISCC 2022), DOI: 10.1109/ISCC55528.2022.9912465
- 18.94. A. Lisi, A. De Salve, P. Mori and L. Ricci. *Selective Disclosure in Self-Sovereign Identity Based on Hashed Values*. In Proceedings of the 2022 IEEE Symposium on Computers and Communications (ISCC 2022), DOI: 10.1109/ISCC55528.2022.9913052
- 18.93. A. De Salve, A. Lisi, P. Mori and L. Ricci. *Measuring EOS.IO DApp resource allocation and costs through a benchmark application*. In Proceedings of the 4th International Conference on Blockchain Technology and Applications (ICBTA 2021), ACM, pp 24-30, DOI: 10.1145/3510487.3510492
- 18.92. S. Bistarelli, F. Faloci, P. Mori. *\*.chain: automatic coding of smart contracts and user interfaces for supply chains*. In proceedings of The Third International Conference on Blockchain Computing and Applications (BCCA2021) (2021), pp 164-171, DOI: 10.1109/BCCA53669.2021.9656987
- 18.91. S. Bistarelli, F. Faloci, P. Mori. *Towards a graphical DSL for tracing supply chains on blockchain*. In proceedings of The 4th International Workshop on Future Perspective of Decentralized Applications (FDAPP2021), held in conjunction with the 27th International European Conference on Parallel and Distributed Computing (EuroPar2021) (2021) Lecture Notes in Computer Science, Springer, vol 13098, pp 219-229, Springer, DOI: 10.1007/978-3-031-06156-1\_18
- 18.90. L. Franceschi, A. Lisi, A. De Salve, P. Mori, L. Ricci. *DART: Towards a role-based trust management system on blockchain*. In Proceedings of the 30th IEEE International Conference on Enabling Technologies for Infrastructure for Collaborative Enterprises (WETICE 2021) (2021), IEEE, pp 75-80, DOI: 10.1109/WETICE53228.2021.00025
- 18.89. A. Lisi, D. Di Francesco Maesa, P. Mori, L. Ricci. *Lightnings over rose bouquets: an analysis of the topology of the Bitcoin Lightning Network*. In Proceedings of COMPSAC 2021: Intelligent and Resilient Computing for a Collaborative World (2021), IEEE, pp 324-331, DOI: 10.1109/COMPSAC51774.2021.00053
- 18.88. A. Lisi, A. De Salve, P. Mori and L. Ricci. *Practical Application and Evaluation of Atomic Swaps for Blockchain-based Recommender Systems*. In Proceedings of the 3rd International Conference on Blockchain Technology and Applications (ICBTA 2020), DOI 10.1145/3446983.3446993, ISBN 978-145038896-2
- 18.87. O. Osliak, A. Saracino, F. Martinelli and P. Mori. *Improving security in Industry 4.0 by extending OPC-UA with Usage Control*. In Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES 2020) DOI 10.1145/3407023.3407077, ISBN 978-145038833-7
- 18.86. A. Lisi, A. De Salve, P. Mori, L. Ricci. *A Smart Contract Based Recommender System*. In Proceedings of the 16th International Conference on the Economics of Grids, Clouds, Systems, and Services (GECON 2019), Lecture Notes in Computer Science 11819, Springer 2019, 29-42, DOI 10.1007/978-3-030-36027-6\_3, ISBN 978-3-030-36026-9
- 18.85. D. Di Francesco Maesa, A. Lunardelli, P. Mori, L. Ricci. *Exploiting Blockchain Technology for Attribute Management in Access Control Systems*. In Proceedings of the 16th International Conference on the Economics of Grids, Clouds, Systems, and Services (GECON2019), 3-14, DOI 10.1007/978-3-030-36027-6\_1, ISBN 978-3-030-36026-9
- 18.84. A. La Marra, F. Martinelli, P. Mori, A. Rizos and A. Saracino. *Using IFTTT to Express and Enforce UCON Obligations*. In Proceedings of the 15th International Conference on Information Security Practice and Experience (ISPEC2019), Lecture Notes in Computer Science 11879, Springer, 213-231, DOI 10.1007/978-3-030-34339-2\_12, ISBN 978-3-030-34339-2, Best Paper Award
- 18.83. A. La Marra, A. Lunardelli, F. Martinelli, P. Mori, A. Saracino, P. Castoldi, F. Marino, B. Martini. *Demonstration of secure slicing using ETSI MANO enhanced with Usage Control*

- Capability*. In Proceedings of the 2019 IEEE Conference on Network Softwarization (NetSoft 2019), 254–256, DOI 10.1109/NETSOFT.2019.8806635, ISBN 978-1-5386-9376-6
- 18.82. P. Castoldi, A. Lunardelli, A. La Marra, F. Marino, F. Martinelli, B. Martini, P. Mori, A. Saracino. *Enhancing Security in ETSI Open Source MANO with Usage Control Capability*. In Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management (IM 2019), 25–29, ISBN 978-3-903176-15-7
- 18.81. F. Di Cerbo, F. Martinelli, P. Mori, A. Saracino. *Obligation Management in Usage Control Systems*. In Proceedings of the 27th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP 2019), IEEE (2019), 356–364, DOI 10.1109/EMPDP.2019.8671586, ISBN 978-1-7281-1644-0
- 18.80. F. Martinelli, C. Michailidou, P. Mori, A. Saracino. *Managing QoS in Smart Buildings Through Software Defined Network and Usage Control*. In Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2019, 626–632, DOI 10.1109/PERCOMW.2019.8730751, ISBN 978-1-5386-9151-9
- 18.79. V. Gkioulos, A. Rizos, C. Michailidou, P. Mori, A. Saracino. *Enhancing Usage Control for Performance: An Architecture for Systems of Systems*. In Computer Security - ESORICS 2018 International Workshops, CyberICPS 2018 and SECPRE 2018, Barcelona, Spain, September 6–7, 2018, Revised Selected Papers, Lecture Notes in Computer Science, vol 11387. Springer (2018), 69–84, DOI 10.1007/978-3-030-12786-2\_5, ISBN 978-3-030-12785-5
- 18.78. V. Gkioulos, A. Rizos, C. Michailidou and P. Mori. *Enhancing Usage Control for Performance: A Proposal for Systems of Systems (Research Poster)*. In Proceedings of the 2018 International Conference on High Performance Computing & Simulation (HPCS 2018), 2018, 1061–1062, DOI 10.1109/HPCS.2018.00169, ISBN 978-1-5386-7878-7
- 18.77. F. Di Cerbo, F. Martinelli, I. Matteucci, P. Mori. *Towards A Declarative Approach to Stateful and Stateless Usage Control for Data Protection*. In Web Information Systems and Technologies - 14th International Conference, WEBIST 2018, Seville, Spain, September 18–20, 2018, Revised Selected Papers, Lecture Notes in Business Information Processing 372, Springer 2019, 308–315, DOI 10.5220/0006962503080315, ISBN 978-3-030-35329-2
- 18.76. G. Costantino, A. La Marra, F. Martinelli, P. Mori, A. Saracino. *Privacy Preserving Distributed Attribute Computation for Usage Control in the Internet of Things*. In Proceedings of the 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications / 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE 2018), IEEE 2018, 1844–1851, DOI 10.1109/TrustCom/BigDataSE.2018.00279, ISBN 978-1-5386-4388-4
- 18.75. D. Di Francesco Maesa, P. Mori, L. Ricci. *Blockchain Based Access Control Services*. In Proceedings of the IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) (iThings/GreenCom/CPSCom/SmartData 2018), 1379–1386, DOI 10.1109/Cybermatics 2018.2018.00237, ISBN 978-1-5386-7975-3
- 18.74. G. Costantino, A. La Marra, F. Martinelli, P. Mori, A. Saracino. *Privacy Preserving Distributed Computation of Private Attributes for Collaborative Privacy Aware Usage Control Systems*. In Proceedings of the 2018 IEEE International Conference on Smart Computing (SMARTCOMP 2018), IEEE Computer Society 2018, 315–320, DOI 10.1109/SMARTCOMP.2018.00022, ISBN 978-1-5386-4705-9
- 18.73. F. Martinelli, C. Michailidou, P. Mori, A. Saracino. *Too Long, did not Enforce: A Qualitative Hierarchical Risk-Aware Data Usage Control Model for Complex Policies in Distributed Environments*. In Proceedings of the 4th ACM Cyber-Physical System Security Workshop (CPSS 2018) held in conjunction with ACM AsiaCCS'18, 27–37, DOI 10.1145/3198458.3198463, ISBN 978-1-4503-5755-5
- 18.72. A. La Marra, F. Martinelli, P. Mori, A. Rizos, A. Saracino. *Improving MQTT by Inclusion of Usage Control*. In Proceedings of the 10th International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage (SpaCCS 2017), Lecture Notes in Computer Science, vol 10656. Springer, Cham (2017), 545–560, DOI 10.1007/978-3-319-72389-1\_43, ISBN 978-3-319-72388-4
- 18.71. A. La Marra, F. Martinelli, P. Mori, A. Rizos, A. Saracino. *Introducing Usage Control in*

- MQTT protocol for IoT*. In Computer Security - ESORICS 2017 International Workshops, CyberICPS 2017 and SECPRE 2017, Oslo, Norway, September 14-15, 2017, Revised Selected Papers. Lecture Notes in Computer Science, vol 10583, Springer, Cham (2017), 35–43, DOI 10.1007/978-3-319-72817-9\_3, ISBN 978-3-319-72816-2
- 18.70. A. De Salve, P. Mori, L. Ricci *Evaluating the Impact of Friends in Predicting User's availability in Online Social Networks*. In Proceedings of the 1st International Workshop on Personal Analytics and Privacy: An Individual and Collective Perspective (PAP2017), held in Conjunction with ECML PKDD 2017 Lecture Notes in Computer Science, vol 10708, Springer (2017), 51–63, DOI 10.1007/978-3-319-71970-2\_6, ISBN 978-3-319-71969-6
- 18.69. G. Giorgi, A. La Marra, F. Martinelli, P. Mori, A. Saracino *Smart Parental Advisory: A Usage Control and Deep Learning-based Framework for Dynamic Parental Control on Smart TV*. In Proceedings of the 13th International Workshop on Security and Trust Management (STM 2017), Lecture Notes in Computer Science, vol 16547, Springer (2017), 118–133, DOI 10.1007/978-3-319-68063-7\_8, ISBN 978-3-319-68062-0
- 18.68. A. La Marra, F. Martinelli, P. Mori, A. Saracino *Implementing Usage Control in Internet of Things: A Smart Home Use Case*. In Proceedings of 2017 16TH IEEE INTERNATIONAL CONFERENCE ON TRUST, SECURITY AND PRIVACY IN COMPUTING AND COMMUNICATIONS / 11TH IEEE INTERNATIONAL CONFERENCE ON BIG DATA SCIENCE AND ENGINEERING / 14TH IEEE INTERNATIONAL CONFERENCE ON EMBEDDED SOFTWARE AND SYSTEMS, Trustcom/BigDataSE/ICISS, IEEE Computer Society 2017, 1056–1063, DOI 10.1109/Trustcom/BigDataSE/ICISS.2017.352, ISBN 978-1-5090-4906-6
- 18.67. D. Di Francesco Maesa, P. Mori, L. Ricci *Blockchain Based Access Control*. In Proceedings of the 17th IFIP WG 6.1 International Conference on Distributed Applications and Interoperable Systems (DAIS2017), Lecture Notes in Computer Science, vol 81036, Springer (2017), 206–220, DOI 10.1007/978-3-319-59665-5\_15, ISBN 978-3-319-59664-8
- 18.66. A. De Salve, B. Guidi, P. Mori, L. Ricci, V. Ambriolo *Privacy and temporal aware allocation of data in Decentralized Online Social Networks*. In Proceedings of the 12th International Conference on Green, Pervasive and Cloud Computing (GPC 2017), Lecture Notes in Computer Science vol 10232, Springer, (2017), 237–251, DOI 10.1007/978-3-319-57186-7\_19, ISBN 978-3-319-57185-0
- 18.65. F. Martinelli, I. Matteucci, P. Mori, A. Saracino *Concurrent History-based Usage Control Policies*. In Proceedings of the 5th International Conference on Model-Driven Engineering and Software Development (MODELSWARD 2017), SciTePress (2017), 657–666, DOI 10.5220/0006232506570666, ISBN 978-989-758-210-3
- 18.64. F. Martinelli, I. Matteucci, P. Mori, A. Saracino *Enforcement of U-XACML History-based Usage Control Policy*. In Proceedings of the 12th International Workshop on Security and Trust Management (STM 2016), Lecture Notes in Computer Science, vol 9876, Springer, (2016), 64–81, DOI 10.1007/978-3-319-46598-2\_5, ISBN 978-3-319-46597-5
- 18.63. M. Faiella, F. Martinelli, P. Mori, A. Saracino and M. Sheikhalisabadi *Collaborative Attribute Retrieval in Environment with Faulty Attribute Managers*. In Proceedings of the 11th International Conference on Availability, Reliability and Security (ARES 2016), IEEE Computer Society, 296–303, DOI 10.1109/ARES.2016.51, ISBN 978-1-5090-0990-9
- 18.62. B. Guidi, A. De Salve, P. Mori, L. Ricci *Distributed Coverage of Ego networks in F2F Online Social Networks*. In Proceedings of the 2016 Intl IEEE Conferences on Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld 2016), IEEE Computer Society 2016, 423–431, DOI 10.1109/UIC-ATC-ScalCom-CBDCom-IoP-SmartWorld.2016.0078, ISBN 978-1-5090-2771-2
- 18.61. A. De Salve, R. Di Pietro, P. Mori, L. Ricci *Logical Key Hierarchy for Groups Management in Distributed Online Social Network*. In Proceedings of the 21st IEEE Symposium on Computers and Communications (ISCC 2016), IEEE Computer Society 2016, 710–717, DOI 10.1109/ISCC.2016.7543820, ISBN 978-1-5090-0679-3
- 18.60. A. De Salve, P. Mori, L. Ricci, Raed Al-Aaridhi, Kalman Graffi *Privacy-preserving Data Allocation in Decentralized Online Social Networks* In Proceedings of the 16th IFIP WG 6.1

- International Conference on Distributed Applications and Interoperable Systems (IFIP DAIS 2016), Lecture Notes in Computer Science, vol 9687, Springer (2016), 47-60, DOI 10.1007/978-3-319-39577-7\_4, ISBN 978-3-319-39576-0
- 18.59. F. Martinelli, P. Mori, A. Saracino. *Enhancing Android Permission through Usage Control: A BYOD Use-Case*. In Proceedings of the 31st ACM Symposium on Applied Computing (SAC 2016), ACM 2016, 2049-2056, DOI 10.1145/2851613.2851797, ISBN 978-1-4503-3739-7
- 18.58. E. Carniani, G. Costantino, F. Marino, F. Martinelli, P. Mori. *Towards a Usage Control based Video Surveillance Framework*. In Proceedings of 24th Euromicro International Conference on Parallel, Distributed and Network-Based Computing (PDP 2016), IEEE Computer Society (2016), 604-608, DOI 10.1109/PDP.2016.64, ISBN 978-1-4673-8776-7
- 18.57. A. De Salve, P. Mori, L. Ricci. *A Privacy-Aware Framework for Decentralized Online Social Networks*. In Proceedings of the 26th International Conference on Database and Expert Systems Applications (DEXA 2015), Lecture Notes in Computer Science, vol 9262, Springer (2015), 479-490, DOI 10.1007/978-3-319-22852-5\_39, ISBN 978-3-319-22851-8
- 18.56. A. Lazouski, F. Martinelli, P. Mori, A. Saracino. *Stateful Usage Control for Android Mobile Devices*. In Proceedings of the 10th International Workshop on Security and Trust Management (STM 2014), in conjunction with ESORICS 2014, Lecture Notes in Computer Science, vol 8743, Springer (2014), 97-112, DOI 10.1007/978-3-319-11851-2\_7, ISBN 978-3-319-11850-5
- 18.55. R. Conti, E. Marzini, A. Spognardi, I. Matteucci, P. Mori, M. Petrocchi. *Improved Automatic Maturity Assessment of Wikipedia Medical Articles (Short Paper)*. The 13th International Conference on Ontologies, DataBases, and Applications of Semantics (ODBASE 2014), OTM Conferences 2014, Lecture Notes in Computer Science, vol 8841, Springer (2014), 612-622, DOI 10.1007/978-3-662-45563-0\_37, ISBN 978-3-662-45562-3
- 18.54. A. Lazouski, G. Mancini, F. Martinelli, P. Mori. *Architecture, Workflows, and Prototype for Stateful Data Usage Control in Cloud*. 5th International Workshop on Data Usage Management (IEESP-DUMA14), An IEEE CS Security & Privacy Workshop (SPW 2014), co-located with the IEEE Symposium on Security and Privacy (SP), IEEE Computer Society (2014), 23-30, DOI 10.1109/SPW.2014.13, ISBN 978-1-4799-5103-1
- 18.53. E. Marzini, P. Mori, S. Di Bona, D. Guerri, M. Lettere, L. Ricci. *A Secure Cloud Manager for the X1.V1 Platform*. In Proceedings of the 27th IEEE International Symposium on Computer-Based Medical Systems (CBMS 2014), IEEE Computer Society 2014, DOI 10.1109/CBMS.2014.125, ISBN 978-1-4799-4435-4
- 18.52. R. Conti, E. Marzini, A. Spognardi, I. Matteucci, P. Mori, M. Petrocchi. *Maturity assessment of Wikipedia medical articles*. In Proceedings of the 27th IEEE International Symposium on Computer-Based Medical Systems (CBMS 2014), IEEE Computer Society 2014, DOI 10.1109/CBMS.2014.69, ISBN 978-1-4799-4435-4
- 18.51. R. Conti, I. Matteucci, P. Mori, M. Petrocchi. *An Expertise-driven Authoring Tool of Privacy Policies for e-Health*. In Proceedings of the 27th IEEE International Symposium on Computer-Based Medical Systems (CBMS 2014), IEEE Computer Society 2014, DOI 10.1109/CBMS.2014.86, ISBN 978-1-4799-4435-4
- 18.50. S. Gnesi, I. Matteucci, C. Moiso, P. Mori, M. Petrocchi, and M. Vesilind. *MyData, Your Data, Our Data: Managing Privacy Preferences in Multi-Subjects Personal Data*. Proceedings of the 2nd Annual Privacy Forum (APF 2014), Lecture Notes in Computer Science, vol 8450, Springer (2014), 154, DOI 10.1007/978-3-319-06749-0\_11, ISBN 978-3-319-06748-3
- 18.49. G.F. Anastasi, E. Carlini, M. Coppola, P. Dazzi, A. Lazouski, F. Martinelli, G. Mancini, P. Mori. *Usage Control in Cloud Federations*. In Proceedings of The International Conference in Cloud Engineering (IC2E 2014), IEEE Computer Society 2014, 141-146, DOI 10.1109/IC2E.2014.58, ISBN 978-1-4799-3766-0
- 18.48. A. Lunardelli, I. Matteucci, P. Mori, M. Petrocchi. *A Prototype for Solving Conflicts in XACML-based e-Health Policies*. In Proceedings of The 26th IEEE International Symposium on Computer-Based Medical Systems (CBMS2013), IEEE Computer Society (2013), 449-452, ISBN 978-1-4799-1053-3, DOI 10.1109/CBMS.2013.6627838, ISBN 978-1-4799-1053-3
- 18.47. L. Krautsevich, A. Lazouski, F. Martinelli, P. Mori, A. Yautsiukhina. *Integration of Quantitative Methods for Risk Evaluation within Usage Control Policies*. In Proceedings of

- The 22nd International Conference on Computer Communications and Networks (ICCCN2013), Nassau, Bahamas, July 30 - August 2, IEEE (2013), 1-8, DOI 10.1109/ICCCN.2013.6614144, ISBN 978-1-4673-5774-6
- 18.46.A. Lazouski, G. Mancini F. Martinelli, P. Mori *Usage Control in Cloud Systems*. In Proceedings of The 7th International Conference for Internet Technology and Secured Transactions (ICITST-2012), Infonomics Society (2012), 202-207, ISBN 978-1-908320-08-7
- 18.45.I. Matteucci, P. Mori, M. Petrocchi *Prioritized Execution of Privacy Policies*. In Proceedings of the 7th International Workshop on Data Privacy Management (DPM2012), Lecture Notes in Computer Science 7731, Springer (2012), 133-145, ISBN 978-3-642-35889-0, 978-3-642-35890-6, DOI 10.1007/978-3-642-35890-6 10
- 18.44.M. Ciampi, G. De Pietro, C. Esposito, M. Sicuranza, P. Mori, A. Gebrehiwot, P. Donzelli: *On Securing Communications among Federated Health Information Systems* In proceedings of The 31st International Conference on Computer Safety, Reliability and Security (SafeComp 2012), Lecture Notes in Computer Science, vol 7613, Springer (2012), 235-246, ISBN 978-3-642-33674-4, DOI 10.1007/978-3-642-33675-1 21
- 18.43.M. Coppola, P. Dazzi, A. Lazouski, F. Martinelli, P. Mori, J. Jensen, I. Johnson, P. Kershaw *The CONTRAIL approach to Cloud Federations* In Proceedings of The International Symposium on Grids and Clouds (ISGC), Proceedings of Science (2012), DOI 10.22323/1.153.0019
- 18.42.A. Lazouski, F. Martinelli, P. Mori *A Prototype for Enforcing Usage Control Policies Based on XACML*. In proceedings of the 9th International Conference on Trust, Privacy and Security in Digital Business (TrustBus'12), Lecture Notes in Computer Science, vol 7449, Springer (2012), 79-92, ISBN 978-3-642-32286-0, DOI 10.1007/978-3-642-32287-7 7
- 18.41.A. Bertolino, S. Daoudagh, F. Lonetti, E. Marchetti, F. Martinelli, P. Mori *Testing of PolPA Authorization Systems*. In Proceedings of the 7th International Workshop on Automation of Software Test (Special Theme: Automation of Security Test) (AST 2012), (2012) IEEE Computer Society (2012), 8-14, DOI 10.1109/IWAST.2012.6228997, ISBN 978-1-4673-1821-1
- 18.40.G. Karopoulos, P. Mori, F. Martinelli *Continuous Authorizations in SIP with Usage Control*. In Proceedings of the 20th Euromicro International Conference on Parallel, Distributed and Network-Based Computing (PDP2012), IEEE Computer Society (2012), 283-287, DOI 10.1109/PDP.2012.81, ISSN 1066-6192, ISBN 978-0-7695-4633-9
- 18.39.M.C. Buzzi, F. Donini, A. Gebrehiwot, A. Lunardelli, C. Lucchesi, P. Mori *Federation and security aspects for the management of the EHR in Italy* In Proceedings of the Second International Conference Advances in New Technologies, Interactive Interfaces and Communicability (ADNTIIC 2011), Lecture Notes in Computer Science, vol 7547, Springer (2011), 26-37, DOI 10.1007/978-3-642-34010-9 3, ISBN 978-3-642-34009-3
- 18.38.I. Matteucci, P. Mori, M. Petrocchi, L. Wiegand *Controlled Data Sharing in E-health* In Proceedings of the First Workshop on Socio-Technical Aspects in Security and Trust (STAST2011) IEEE (2011), 17-23, ISBN 978-1-4577-1181-7, DOI 10.1109/STAST.2011.6059251
- 18.37.P. Mori, F. Martinelli: *Distributed Authorization System with Mobile Usage Control Policies*. In Proceedings of Computer Aided Systems Theory (EUROCAST 2011) Part I, Lecture Notes in Computer Science, vol 6927, Springer (2011), 56-63, ISBN 978-3-642-27548-7, DOI 10.1007/978-3-642-27549-4 8
- 18.36.G. Gheorghe, P. Mori, B. Crispo, F. Martinelli *Enforcing UCON Policies on the Enterprise Service Bus*. In Proceedings of On the Move to Meaningful Internet Systems 2010 - Confederated International Conference on ePIS, IS, DOA and ODBASE, Part II, Lecture Notes in Computer Science, vol 6427, Springer (2010), 876-893, ISBN 978-3-642-16948-9, DOI 10.1007/978-3-642-16949-6 14
- 18.35.L. Krautsevich, A. Lazouski, F. Martinelli, P. Mori, A. Yautsiukh *Usage Control, Risk and Trust* In Proceedings of the 7th International Conference on Trust, Privacy & Security in Digital Business (TRUSTBUS'10) Lecture Notes in Computer Science, vol 6264, Springer (2010), ISBN 978-3-642-15151-4, DOI 10.1007/978-3-642-15152-1 1
- 18.34.M. Colombo, F. Martinelli, P. Mori, B. Martini, F. Baroncelli, P. Castorini *Resource access in Multi-Provider Networks using Role Based Trust Management* In Proceedings of the 5th International Workshop on Security and Trust Management (STM 2009), in conjunction with

- ESORICS 2009, Saint Malo, France, September 24-25, 2009.
- 18.33.A. Lazouski, M. Colombo, F. Martinelli, P. Mori: *A proposal on enhancing XACML with continuous usage control features*. In Proceedings of CoreGRID ERCIM Working Group Workshop on Grids, P2P and Service computing, in conjunction with EuroPAR 2009, Delft, Netherlands, August 24, 2009, Springer US (2010), 133-146, ISBN: 978-1-4419-6794-7, DOI: 10.1007/978-1-4419-6794-7\_11
  - 18.32.P. Mori, S. Naqvi: *Security and Trust Management for Virtual Organisations: GridTrust Approach*. In Proceedings of the 3rd IFIP WG 11.11 International Conference on Trust Management (TM'09), West Lafayette, IN, USA, June 2009. Advances in Information and Communication Technology (AICT) 300 Springer, (2009), 306-309, ISBN 978-3-642-02055-1, DOI 10.1007/978-3-642-02056-8\_21
  - 18.31.A. Lazouski, M. Colombo, F. Martinelli, P. Mori: *On Usage Control for GRID Services*. In Proceedings of the Second International Joint Conference on Computational Sciences and Optimization (CSO 2009), The 2009 IEEE International Workshop on HPC and Grid Applications (IWHGA2009), Sanya, Hainan Island, China, 24-26 April 2009, Volume 1, IEEE Computer Society, ISBN 978-0-7695-3605-7, DOI 10.1109/CSO.2009.479
  - 18.30.S. Naqvi, P. Massonet, B. Aziz, A. Arenas, F. Martinelli, P. Mori, L. Blasi, G. Cortese: *Fine-grained Continuous Usage Control of Service based Grids - The GridTrust Approach*. In proceedings of Towards a Service-Based Internet, First European Conference (ServiceWave 2008), Madrid, Spain, December 10-13, 2008. Lecture Notes in Computer Science, vol 5377, Springer (2008), 242-253, ISBN 978-3-540-89896-2, DOI 10.1007/978-3-540-89897-9\_21
  - 18.29.A. Castrucci, F. Martinelli, P. Mori, F. Ropert: *Enhancing Java ME Security Support with Resource Usage Monitoring*. In proceedings of the 10th International Conference on Information and Communications Security (ICICS08), Birmingham, UK, October 20-22, 2008. Lecture Notes in Computer Science, vol 5308, Springer Verlag (2008) 256-266, ISBN 978-3-540-88624-2, DOI 10.1007/978-3-540-88625-9\_17
  - 18.28.B. Aziz, A. Arenas, F. Martinelli, I. Matteucci P. Mori: *Controlling Usage of Business Processes through Fine-Grained Security Policies*. In proceedings of the 5th International Conference on Trust, Privacy and Security in Digital Business (TrustBus08), Turin, Italy, September 4-5, 2008. Lecture Notes in Computer Science, vol 5185, Springer Verlag (2008) 100-117, ISBN 978-3-540-85734-1, DOI 10.1007/978-3-540-85735-8\_11
  - 18.27.L. Blasi, A. Arenas, B. Aziz, P. Mori, U. Rovati, B. Crispo, F. Martinelli, P. Massonet: *Secure Environment for Grid-Based Supply Chains*. Collaboration and the Knowledge Economy: Issues, Applications, Case Studies (eChallenge08), Stockholm, Sweden, October, 22-14, 2008. P. and M. Cunningham (Eds), IOS Press (2008) Amsterdam, ISBN 978-1-58603-924-0
  - 18.26.F. Martinelli, P. Mori, T. Quillinan and C. Schaefer: *A Runtime Monitoring Environment for Mobile Java*. In proceedings of the 1st International ICST workshop on Security Testing (SecTest08), Lillehammer, Norway, April, 9, 2008. International Conference on Software Testing Verification and Validation Workshop, 2008 (ICSTW '08), IEEE Computer Society 2008, 270-278, DOI 10.1109/ICSTW.2008.3, ISBN 978-0-7695-3388-9
  - 18.25.M. Colombo, F. Martinelli, P. Mori, M. Petrocchi and A. Vaccaro: *Fine Grained Access Control with Trust and Reputation Management for Globus*. In Proceeding of On the Move to Meaningful Internet System 2007 (topIS, DOA, GADA, and ODBASE: Lecture Notes in Computer Science, vol 4804, Springer Verlag (2007) 1505-1515, ISBN-10 3-540-76835-1, ISBN-13 978-3-540-76835-7, ISSN 0302-9743, DOI 10.1007/978-3-540-76843-2\_26
  - 18.24.F. Martinelli and P. Mori: *A Model for Usage Control in GRID Systems*. In Proceedings of the Third International Conference on Security and Privacy in Communications Networks and the Workshops, 2007. Grid-STP 2007, International Workshop on Security, Trust and Privacy in Grid System SecureComm 2007, IEEE Press (2007), 169-175, IEEE Catalog Number: 07EX1681, ISBN: 1-4244-0975-6, DOI 10.1109/SECCOM.2007.4550326
  - 18.23.M. Colombo, F. Martinelli, P. Mori and A. Vaccaro: *Extending the Globus architecture with Role-Based Trust Management*. In Proceeding of the Eleventh International Conference on Computer Aided Systems Theory (Eurocast 2007) Lecture Notes in Computer Science, 4739, Springer Verlag (2007) 448-456, ISBN-10 3-540-75866-6, ISBN-13 978-3-540-75866-2, ISSN 0302-9743, DOI 10.1007/978-3-540-75867-9\_57
  - 18.22.H. Koshutanski, F. Martinelli, P. Mori, L. Borz and A. Vaccaro: *A Fine Grained and X.509*

- Based Access Control System for Globus*. In Proceeding of On the Move to Meaningful Internet System 2006 (CoopIS, DOA, GADA, and ODBASE: Lecture Notes in Computer Science, vol 4276, Springer Verlag (2006) 1336–1350, ISBN-10 3-540-48274-1, ISBN-13 978-3-540-48274-1, ISSN 0302-9743, DOI 10.1007/11914952 21
- 18.21. H. Koshutanski, F. Martinelli, P. Mori and A. Vaccarelli: *Fine-grained and History-based Access Control with Trust Management for Autonomic Grid Services*. In Proceedings of International Conference on Autonomic and Autonomous Systems (ICAS06) IEEE Computer Society (2006) 34, Best Paper Award, ISBN 0-7695-2653-5, DOI 10.1109/ICAS.2006.25
- 18.20. F. Baiardi, P. Mori, L. Ricci and A. Vaccarelli: *Short Paper: Policy Driven Virtual Machine Monitor for Protected Grids*. In Proceedings of the 15th IEEE International Symposium on High Performance Distributed Computing (HPDC 2006) IEEE Computer Society (2006) 313–316, ISBN 1-4244-0307-3, ISSN 1082-8907, DOI 10.1109/HPDC.2006.1652164
- 18.19. F. Martinelli, P. Mori and A. Vaccarelli: *Towards Continuous Usage Control on Grid Computational Services*. In Proceedings of Joint International Conference on Autonomic and Autonomous Systems and International Conference on Networking and Services (ICAS-ICNS 2005) IEEE Computer Society (2005) 82, DOI 10.1109/ICAS-ICNS.2005.93, ISBN 0-7695-2450-8.
- 18.18. F. Baiardi, P. Mori and L. Ricci: *Solving Irregular Problems through Parallel Irregular Trees*. In Proceeding of The IASTED International Conference on Parallel and Distributed Computing and Networks (PDCN 2005), part of the 23rd Multi-Conference on Applied Informatics, IASTED/ACTA Press 2005, T. Fahringer and M.H. Hamza (2005) 246–251, ISBN 0-88986-470-5
- 18.17. F. Baiardi, F. Martinelli, P. Mori, and A. Vaccarelli: *Improving Grid Service Security with Fine Grain Policies*. In Proceeding of On the Move to Meaningful Internet System 2004: OTM Workshops, Lecture Notes in Computer Science, vol 3292, Springer Verlag (2004) 123–134, DOI 10.1007/978-3-540-30470-8 30 ISBN: 978-3-540-23664-1
- 18.16. F. Baiardi, P. Mori and L. Ricci: *Parallel Hierarchical Radosity: the PIT Approach*. In Proceedings of Workshop on State-Of-The-Art in Scientific Computing (PARA 2004), Lecture Notes in Computer Science, vol 3732, Springer Verlag (2004) 1031–1040, DOI 10.1007/11558958 125, ISBN 3-540-29067-2
- 18.15. F. Baiardi, D. Guerri, P. Mori, L. Ricci and L. Vaglin: *MPI on a Virtual Shared Memory*. In proceedings of Parallel Computing Software Technology, Algorithms, Architectures and Applications (PARCO), in Advances in Parallel Computing, Volume 13, Joubert, Nagel, Peters, Walter eds, Elsevier Press (2004) 169–176, ISBN 0-444-51689-1
- 18.14. F. Baiardi, A. Bonotti, L. Ferrucci, P. Mori and L. Ricci: *Load Balancing by Domain Decomposition: the Bounded Neighbour Approach*. In Proceedings of the 17th European Simulation Multiconference, SCS European Publishing House (2003) 371–377
- 18.13. F. Baiardi, P. Mori and L. Ricci: *A JAVA Support for Distributed Shared Memory on COW*. In Proceedings of the 20th IASTED International Conference Applied Informatics, International Symposium on Parallel and Distributed Computing and Networks (AI 2002), M. H. Hamza ed. (2002) 191–195
- 18.12. D. Guerri, P. Mori, L. Ricci, F. Baiardi and L. Vaglin: *MPI SH: a Distributed Shared Memory Implementation of MPI*. In Proceedings of the 4th International Conference on Massively Parallel Computing Systems, National Technological University Press, Colorado, USA (2002) 129–134
- 18.11. F. Baiardi, P. Mori and L. Ricci: *PIT: A Library for the Parallelization of Irregular Problems*. In Proceedings of the 6th International Conference on Applied Parallel Computing (PARA 2002), Lecture Notes in Computer Science, vol 2367, Springer Verlag (2002) 185–194, DOI 10.1007/3-540-48051-X 19, ISBN 3-540-43786-X
- 18.10. P. Mori and L. Ricci: *Computational Science In High School Curricula: The ORESPICS Approach*. In Proceedings of International Conference on Computational Science (ICCS 2002), Lecture Notes in Computer Science 2331, Springer Verlag (2002) 898–907, DOI 10.1007/3-540-47789-6 94, ISBN 3-540-43594-8
- 18.9. F. Baiardi, P. Mori and L. Ricci: *Collecting Remote Data in Irregular Problems with Hierarchical Representation of the Domain*. In Proceedings of Recent Advances in Parallel Virtual Machine and Message Passing Interface, 8th European PVM/MPI Users' Group

- Meeting (2001), Lecture Notes in Computer Science 2131, Springer Verlag (2001) 304-310, DOI 10.1007/3-540-45417-9 42, ISBN 3-540-42609-4
- 18.8.F. Baiardi, D. Guerri, P. Mori, L. Moroni and L. Ricci *Two Layers Distributed Shared Memory*. In Proceedings of High-Performance Computing and Networking, 9th International Conference, HPCN Europe 2001, Lecture Notes in Computer Science, vol 2110, Springer Verlag (2001) 302-311, DOI 10.1007/3-540-48228-8 31, ISBN 3-540-42293-5
- 18.7.F. Baiardi, D. Guerri, P. Mori, L. Moroni and L. Ricci *DVSA and SHOB: Support to Shared Data Structures on Distributed Memory Architectures*. In Proceedings of the 9th Euromicro Workshop on Parallel and Distributed Processing 2001 (Euro PDP2001), IEEE Computer Society (2001) 165-172, DOI 10.1109/EMPDP.2001.905039, ISBN 0-7695-0987-8
- 18.6.F. Baiardi, G. Doblioni, P. Mori and L. Ricci *Hive: Implementing a Virtual Distributed Shared Memory in Java*. In Proceedings of DAPSYS - 3rd Austrian Hungarian Workshop on Distributed and Parallel Systems, P. Kacsus, G. Kotsis eds, Kluwer Academic Publishers, Norwell, MA, USA, (2000) 169-172, ISBN 978-1-4615-4489-0
- 18.5.F. Baiardi, S. Chiti, P. Mori and L. Ricci *Adaptive Multigrid Methods in MPI*. In Proceedings of Euro PVM/MPI 2000, Lecture Notes in Computer Science, vol 1908, Springer Verlag (2000) 80-87, DOI 10.1109/EMPDP.2000.823425, ISBN 3-540-41010-4
- 18.4.F. Baiardi, P. Becuzzi, S. Chiti, P. Mori and L. Ricci *A Hierarchical Approach to Irregular Problems*. In Proceedings of Europar 2000, Lecture Notes in Computer Science 1900, Springer Verlag (2000) 218-222, DOI 10.1007/3-540-44520-X 30, ISBN 3-540-67956-1
- 18.3.F. Baiardi, S. Chiti, P. Mori and L. Ricci *Parallelization of Irregular Problems Based on Hierarchical Domain Representation*. In Proceedings of the 8th International Conference on High Performance Computing and Networking (HPCN EUROPE 2000), Lecture Notes in Computer Science, vol 1823, Springer Verlag (2000) 71-80, DOI 10.1007/3-540-44520-X 30, ISBN 3-540-67553-1
- 18.2.F. Baiardi, D. Guerri, P. Mori and L. Ricci *Evaluation of a Virtual Shared Memory by the Compilation of Data Parallel Loops*. In Proceedings of the 8th Euromicro Workshop on Parallel and Distributed Processing (Euro PDP2000), IEEE Computer Society (2000) 309-316, DOI 10.1109/EMPDP.2000.823425, ISBN 0-7695-0500-7
- 18.1.F. Baiardi, P. Becuzzi, P. Mori and M. Paolucci *Load balancing and locality in hierarchical n-body algorithms on distributed memory architectures*. In Proceedings of the 6th International Conference on High Performance Computing and Networking (HPCN EUROPE 1998), Lecture Notes in Computer Science, vol 1401, Springer Verlag (1998) 284-293, DOI 10.1007/BFb0037155, ISBN 3-540-64443-1
- 19. Capitoli di Libri**
- 19.15.O. Osliak, P. Mori, A. Saracino *Usage Control for Industrial Control System*. Collaborative Approaches for Cyber Security in Cyber-Physical Systems, Advanced Sciences and Technologies for Security Applications, Springer, Cham, 191-207, (2023), DOI 10.1007/978-3-031-16088-2 9
- 19.14.A. La Marra, F. Martinelli, P. Mori, A. Saracino *A Distributed Usage Control Framework for Industrial Internet of Things*. Security and Privacy Trends in the Industrial Internet of Things, Springer, 115-135, (2019), DOI 10.1007/978-3-030-12330-7 6, ISBN 978-3-030-12329-1
- 19.13.F. Di Cerbo, A. Lunardelli, F. Martinelli, I. Matteucci, P. Mori *A Declarative Data Protection Approach: From Human-Readable Policies to Automatic Enforcement* In 14th Conference on International Web Information Systems and Technologies (WEBIST 2018) Revised Selected Papers, Lecture Note in Business Information Processing 372, Springer (2019), 78-89, DOI 10.1007/978-3-030-35330-8 5, ISBN 978-3-030-35330-8
- 19.12.M. Egea, I. Matteucci, P. Mori, M. Petrocchi *Definition of Data Sharing Agreements (The case of Spanish Data Protection Law)*. In Accountability and Security in the Cloud - First Summer School, Cloud Accountability Project, A4Cloud, Lecture Notes in Computer Science, vol 8937, Springer, (2015), 248-270, DOI 10.1007/978-3-319-17199-9 11, ISBN 978-3-319-17198-2
- 19.11.G. Costa, A. Lazouski, F. Martinelli and P. Mori *Application Security for Mobile Devices*. Handbook of Research on Innovations in Systems and Software Engineering, IGI Global, (2014), 562-588 DOI 10.4018/978-1-4666-6359-6.ch022, ISBN 978-1-4666-6359-6

- 19.10. R. Conti, A. Lunardelli, I. Matteucci, P. Mori, M. Petrocchi and M. Wilso: *Preserving Data Privacy in eHealth*. In M. Heisel et al. (Eds.): *Engineering Secure Future Internet Services*, Lecture Notes in Computer Science, vol 8431, 366-392, Springer International Publishing Switzerland (2014), DOI 10.1007/978-3-319-07452-8\_15, ISBN 978-3-319-07451-1
- 19.9. M.C. Buzzi, E. Cesario, M. Ciampi, G. De Pietro, F. Folino, P. Mori, M. Sicuranza, P. Storniolo, D. Talia, A. Ursola: *Linee Guida per il Cloud in Sanità*. Documentalia, CNR (2013)
- 19.8. M.C. Buzzi, F. Donini, A. Gebrehiwot, A. Lunardelli, C. Lucchesi, P. Morici: *Italian Electronic Health Record: a proposal of a Federated Authentication and Authorization Infrastructure*. New Horizons in Creative Open Software, Multimedia, Human Factors and Software Engineering, Blue Herons Editions (2012) 678-681, DOI:10.978.8896471/012, ISBN 978-88-96471-01-2
- 19.7. G. Costa, A. Lazouski, F. Martinelli and P. Mori: *Application Security for Mobile Devices. Dependability and Computer Engineering Concepts for Software-Intensive Systems*. Editors L. Petre, K. Sere, and E. Troubitsyna, IGI Global (2012) 266-284. DOI:10.4018/978-1-60960-747-0.ch012, ISBN 978-1-60960-747-0
- 19.6. B. Martini, P. Mori, F. Martinelli, A. Lazouski, P. Castoldi: *Time-continuous Authorization of Network Resources based on Usage Control*. In Trustworthy Internet, L. Salgarelli et al. eds. Springer-Verlag (2011), 235-245, DOI 10.1007/978-88-470-1818-1\_18, ISBN 978-88-470-1817-4
- 19.5. B. Aziz, A. Arenas, F. Martinelli, P. Mori, M. Petrocchi and M. Wilso: *Trust Management for Grid Systems. Trust Modeling and Management in Digital Environments*. Editor Social Concept to System Development Editor Zheng Yan, IGI Global (2010) 149-170, DOI: 10.4018/978-1-61520-682-7.ch007, ISBN 978-1-615-20682-7
- 19.4. M. Colombo, A. Lazouski, F. Martinelli and P. Mori: *Access and Usage Control in GRID Systems. Handbook on Information and Communication Security*. Editor Peter P. Stavroulakis, Mark Stamp, Springer (2010) 293-318, ISBN 978-3-642-04117-4, DOI 10.1007/978-3-642-04117-4\_16
- 19.3. N. Dragoni, F. Martinelli, F. Massacci, P. Mori, C. Schaefer, T. Walter and E. Vetillard: *Security-by-Contract (SxC) for Software and Services of Mobile Systems*. At Your service: Service-Oriented Computing from and EU Perspective. Wiley (2009) 429-455, ISBN 978-0-262-04253-6
- 19.2. P. Massonet, A. Arenas, F. Martinelli, P. Mori and B. Cristofari: *GridTrust-A Usage Control-Based Trust and Security Framework for Service-Based Grids*. At Your service: Service-Oriented Computing from and EU Perspective. Wiley (2009) 407-421, ISBN 978-0-262-04253-6
- 19.1. F. Martinelli and P. Mori: *Enhancing Java Security with History Based Access Control*. Foundations of Security Analysis and Design, Tutorial Lectures (FOSAD 2006/2007). Lecture Notes in Computer Science, vol 4577, Springer Verlag (2007) 135-159, DOI 10.1007/978-3-540-74810-6\_5, ISBN 978-3-540-74809-0
- 20. Altre Pubblicazioni**
- 20.5. D. Albanese, G. Crincoli, M. De Vincenzi, G. Iadarola, F. Martinelli, I. Matteucci, P. Mori: *Privacy-Preserving Data Sharing for Collaborative Analytics in Multi-Modal Transportation Systems*. ERCIM News 133, 21-22, Special theme Data Infrastructures and Management, aprile 2023
- 20.4. D. Di Francesco Maesa, P. Mori, L. Ricci: *Distributed Access Control Through Blockchain Technology*. ERCIM News 110, 31-32, luglio 2017
- 20.3. P. Mori, A. Saracino, F. Di Cerbo: *Data Usage Control: Introducing a New Framework for Cloud and Mobile Environments*. ERCIM News 106, 30-31, luglio 2016
- 20.2. G. Costa, F. La Torre, F. Martinelli, P. Mori: *Parental Control for Mobile Devices*. ERCIM News 82, 61-62, luglio 2010
- 20.1. F. Martinelli, F. Massacci, P. Mori, C. Schaefer, T. Walter: *Enhancing Java ME Security Support with Resource Usage Monitoring*. ERCIM News 75, ottobre 2008
- 21. Rapporti Tecnici**
- 21.6. F. Martinelli, I. Matteucci, P. Mori, A. Bertolino, A. Calabro, F. Di Giandomenico, G. Lami,

F. Lonetti, E. Marchetti: *Secure Software Engineering for Connected Vehicles* A Research Agenda. Technical report IIT-TR-18-2015.

21.5.A. Lazouski, G. Mancini, F. Martinelli, P. Mori: *Usage Control in Cloud Systems* Technical report IIT TR-06/2012

21.4.A. Lazouski, F. Martinelli, P. Mori: *A Survey of Usage Control in Computer Security* Technical report IIT TR-12/2008

21.3.F. Martinelli and P. Mori: *On Usage Control for GRID Systems*. Technical report IIT TR-01/2008

21.2.F. Martinelli, P. Mori and A. Vaccarella: *Fine Grained Access Control for Computational Services*. Technical report IIT TR-06/2006

21.1.M. Colombo, F. Martinelli, P. Mori and A. Vaccarella: *Extending the Globus architecture with Role-Based Trust Management*. Technical report IIT TR-05/2006

## 22. **Contributi a Documenti**

22.1. Raccomandazione e Proposte sull'Utilizzo del Cloud Computing nella Pubblica Amministrazione. Versione 2.0 del 28 giugno 2012. Disponibile all'indirizzo: [https://www.agid.gov.it/sites/default/files/repository\\_files/documenti\\_indirizzo\\_raccomandazioni\\_cloud\\_e\\_pa\\_-2.0\\_0.pdf](https://www.agid.gov.it/sites/default/files/repository_files/documenti_indirizzo_raccomandazioni_cloud_e_pa_-2.0_0.pdf)

22.2. Scheda del Key Topic "Data Ownership" del documento "Digitalisation of the Manufacturing Sector: Opportunities and challenges for the Italian Industry", Cluster Tecnologico Nazionale Fabbrica Intelligente

## 23. **Invited Talks**

23.11. *Blockchain e Tracciabilit a*. Cybersecurity Day 2023, Internet Festival 2023, Pisa, Italia, 06 ottobre 2023.

23.10. *Blockchain e Sistemi di Raccomandazione, Access Control su Blockchain*, evento "Scatena la tua Ricerca con la Blockchain", presso Istituto Superiore per la Protezione e la Ricerca Ambientale (ISPRA), Roma, Italia, 18 Febbraio 2020

23.9. *Blockchain Based Domain Auctions*. 15th CENTR R&D Workshop, Pisa, Italia, 27 Novembre 2019

23.8. *Data Usage Control in Cloud and IoT*. Conferenza del Dipartimento DIITET del CNR, Area Strategica "Informatica", Pisa, Italia, 30 novembre 2018

23.7. *IoT and Data Protection*. Cybersecurity Day 2018, Internet Festival 2018, Pisa, Italia, 12 ottobre 2018.

23.6. *Blockchain based Access Control*. Distributed Ledger Technology Workshop: Challenges and perspectives in the technological, scientific, social and economic fields degli Studi di Perugia, Perugia, 1 febbraio 2018

23.5. *Usage Control on Cloud and Mobile Devices: the Coco Cloud Approach*. 2015 CSecLab Workshop on Security of Mobile Applications, Genova, Italia, 12 novembre 2015

23.4. *Usage control in Cloud/Mobile systems*. Workshop of Cyber Security Technological District. Rende (CS), Italia, 4-5 novembre 2014

23.3. *Usage control in CONTRAIL Cloud*. Cyber Security & Privacy EU Forum 2012 (CSP EU Forum). Berlin, Germany, 24-25 aprile 2012.

23.2. *Usage control in CONTRAIL Cloud*. International Workshop on Policy for the Future Internet 2011, Colocated with IEEE International Symposium on Policies for Distributed Systems and Networks. Pisa, Italia, 9 giugno 2011.

23.1. ESFORs 2006: European Security Forum for Web Services, Software and Systems. Paris, France, 6-7 settembre 2006.

## 24. **Demo**

24.7. Italian Innovation Day 2018, EIT Digital Private Virtual Federator demo, Trento, Italia, 29 novembre 2018

24.6. Italian Innovation Day 2016, EIT Digital Trusted Data Management with Service Ecosystem HII, Catalysts 1605 demo, Trento, Italia, 15 dicembre 2016

24.5. Internetdagarna 2016, EIT Digital Trusted Data Management with Service Ecosystem HII,

- Catalysts 1605 and 1639 demos, Stockholm, Sweden, 22 novembre 2016
- 24.4. Italian Innovation Day 2015, EIT Digital Trusted Data Management with Service Ecosystem HII, Catalyst 1511 demo, Trento, Italia, 10 dicembre 2015
- 24.3. EIT Digital Results Day Finland, EIT Digital Trusted Data Management with Service Ecosystem HII, Catalyst 1511 demo, Helsinki, Finland, 1 dicembre 2015
- 24.2. The 3rd IFIP International Conference on Trust Management (TMW03), West Lafayette, IN, USA, 19 giugno 2009.
- 24.1. At your serviceservice-oriented demonstrations from IST-PR6, Brussels, Belgium, 26 maggio 2006.

## 25. **Attività Editoriale**

- 25.25. Roberto Di Pietro, Karen Renaud, Paolo Mori Proceedings of the 11th International Conference on Information Systems Security and Privacy, ICISSP 2025 - Volume 2, Porto, Portugal, February 20-22, 2025, CITEPRESS 2025, ISBN 978-989-758-735-1
- 25.24. Special Issue on Advances in Distributed Ledger Technology and its Applications, Blockchain: Research and Applications Paolo Mori, Ivan Visconti, Stefano Bistarelli Laura Ricci, Elsevier B.V. on behalf of Zhejiang University Press, 2024, ISSN: 2096-7209
- 25.23. Gabriele Lenzini, Paolo Mori, Steven Furnell Proceedings of the 10th International Conference on Information Systems Security and Privacy, ICISSP 2024, Rome, Italy, February 26-28, 2024, CITEPRESS 2024, ISBN 978-989-758-683-5
- 25.22. Special Issue on Blockchain Technology and Applications, Pervasive and Mobile Computing. Paolo Mori (Lead Guest Editor), Wolfgang Prinz, Laura Ricci, and Edgard Weippl (Guest editors), vol 71, Elsevier, 2021, <https://www.sciencedirect.com/journal/pervasive-and-mobile-computing/special-issue/10HG7QBDGK> (Dichiarazione prot IIT00574-2020 del 11/09/2020)
- 25.21. Paolo Mori, Ivan Visconti, Stefano Bistarelli Proceedings of the Fifth Distributed Ledger Technology Workshop (DLT 2023), Bologna, Italy, May 25-26, 2023, Workshop Proceedings 3460, CEUR-WS.org 2023
- 25.20. Paolo Mori, Gabriele Lenzini, Steven Furnell Proceedings of the 9th International Conference on Information Systems Security and Privacy, ICISSP 2023, Lisbon, Portugal, February 22-24, 2023, SciTePress 2023, ISBN 978-989-758-624-8
- 25.19. Emerging Technologies for Authorization and Authentication, 5th International Workshop, ETAA 2022, Copenhagen, Denmark, September 30, 2022, Proceedings Andrea Saracino, Paolo Mori (eds). Lecture Notes in Computer Science 13782, Springer 2023, ISBN 978-3-031-25466-6
- 25.18. Paolo Mori, Gabriele Lenzini, Steven Furnell Proceedings of the 8th International Conference on Information Systems Security and Privacy, ICISSP 2022, Online Streaming, February 9-11, 2022, CITEPRESS 2022, ISBN 978-989-758-553-1
- 25.17. Steven Furnell, Paolo Mori, Edgar R. Weippl, Olivier Camarero Information Systems Security and Privacy - 6th International Conference, ICISSP 2020, Valletta, Malta, February 25-27, 2020, Revised Selected Papers Communications in Computer and Information Science 1545, Springer 2022, ISBN 978-3-030-94899-3
- 25.16. Emerging Technologies for Authorization and Authentication, 5th International Workshop, ETAA 2021, Proceedings Andrea Saracino, Paolo Mori (eds). Lecture Notes in Computer Science 13136, Springer 2021
- 25.15. Paolo Mori, Gabriele Lenzini, Steven Furnell Proceedings of the 7th International Conference on Information Systems Security and Privacy, ICISSP 2021, Online Streaming, February 11-13, 2021, CITEPRESS 2021, ISBN 978-989-758-491-6
- 25.14. Emerging Technologies for Authorization and Authentication, 4th International Workshop, ETAA 2020, Guildford, UK, September 18, 2020, Proceedings Andrea Saracino, Paolo Mori (eds). Lecture Notes in Computer Science 12515, Springer 2020, ISBN 978-3-030-64454-3
- 25.13. Steven Furnell, Paolo Mori, Edgar R. Weippl, Olivier Camarero Proceedings of the 6th International Conference on Information Systems Security and Privacy, ICISSP 2020, Valletta, Malta, February 25-27, 2020, CITEPRESS 2020, ISBN 978-989-758-399-5
- 25.12. Paolo Mori, Steven Furnell, Olivier Camarero Information Systems Security and Privacy - 5th

- International Conference, ICISSP 2019, Prague, Czech Republic, February 23-25, 2019, Revised Selected Papers, Communications in Computer and Information Science 1221, Springer 2020, ISBN 978-3-030-49442-1
- 25.11. Emerging Technologies for Authorization and Authentication Second International Workshop, ETAA 2019, Luxemburg, September 27, Proceedings, Giacino and P. Mori (eds.): ETAA 2019, Lecture Notes in Computer Science 11967, Springer Nature Switzerland AG 2019, ISBN 978-3-030-39749-4
- 25.10. Paolo Mori, Steven Furnell, Olivier Camp Proceedings of the 5th International Conference on Information Systems Security and Privacy, ICISSP 2019, Prague, Czech Republic, February 23-25, 2019, SciTePress 2019, ISBN 978-989-758-359-9
- 25.9. Paolo Mori, Massimo Bartoletti, Stefano Bistarelli Proceedings of the Second Distributed Ledger Technology Workshop, DLT@ITASEC 2019, Pisa, Italy, February 12, 2019, Workshop Proceedings 2334, CEUR-WS.org 2019
- 25.8. Emerging Technologies for Authorization and Authentication First International Workshop, ETAA 2018, Barcelona, Spain, September 7, 2018, Proceedings, Giacino and P. Mori (eds.): ETAA 2018, Lecture Notes in Computer Science 11963, Springer Nature Switzerland AG 2018, ISBN 978-3-030-04371-1
- 25.7. Information Systems Security and Privacy - 4th International Conference (ICISSP 2018), Funchal, Madeira, Portugal, January 22-24, 2018, Revised Selected Papers, Communications in Computer and Information Science 977, Mori, Paolo, Furnell, Steven, Camp, Olivier (Eds.), Springer 2019, ISBN 978-3-030-25108-6
- 25.6. Paolo Mori, Steven Furnell, Olivier Camp Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018), Funchal, Madeira - Portugal, January 22-24, 2018, SciTePress 2018, ISBN 978-989-758-282-0
- 25.5. Information Systems Security and Privacy Third International Conference, ICISSP 2017, Porto, Portugal, February 19-21, 2017, Revised Selected Papers, Communications in Computer and Information Science 867, Mori, Paolo, Furnell, Steven, Camp, Olivier (Eds.), Springer, ISBN 978-3-319-93353-5, ebook ISBN 978-3-319-93354-2
- 25.4. O. Camp, S. Furnell, P. Mori Proceedings of the 3rd International Conference on Information Systems Security and Privacy (ICISSP 2017), Porto, Portugal, February 19-21, 2017, SCITEPRESS 2017, ISBN: 978-989-758-209-7
- 25.3. Information Systems Security and Privacy Second International Conference, ICISSP 2016, Rome, Italy, February 19-21, 2016, Revised Selected Papers, Communications in Computer and Information Science Camp, Olivier, Furnell, Steven, Mori, Paolo (Eds.), Springer, ISBN 978-3-319-54432-8, ebook ISBN 978-3-319-54433-5
- 25.2. O. Camp, S. Furnell, P. Mori Proceedings of the 2nd International Conference on Information Systems Security and Privacy (ICISSP 2016), Rome, Italy, February 19-21, 2016, SCITEPRESS 2016, ISBN 978-989-758-167-0
- 25.1. I. Matteucci, P. Mori, M. Petrocchi 1st IEEE/ACM International Workshop on Technical and Legal aspects of data privacy and Security (TELERISE 2015), Florence, Italy, May 18, 2015, IEEE Computer Society 2015, ISBN 978-1-4673-7097-4
- 26. Organizzazione Conferenze e Workshop Internazionali**
- 26.11. General chair della 12th International Conference on Information Systems Security and Privacy (ICISSP 2026), Marbella, Spain, 2026
- 26.10. General co-chair della IEEE International Conference on Blockchain and Cryptocurrency, Pisa, Italy, 2025
- 26.9. General chair della 11th International Conference on Information Systems Security and Privacy (ICISSP 2025), Porto, Portugal, 2025
- 26.8. Program Co-chair del 5th Distributed Ledger Technology Workshop (DLT 2023), 2023
- 26.7. Program Chair della International Conference on Information Systems Security and Privacy (ICISSP)
- 10th edition, Rome, Italy, 2024
  - 9th edition, Lisbon, Portugal, 2023
  - 8th edition, online streaming, 2022

- 7th edition, online streaming, 2021
  - 6th edition, La Valletta, Malta, 2020
  - 5th edition, Prague, Czech Republic, 2019
  - 4th edition, Funchal, Madeira, Portugal, 2018
  - 3rd edition, Porto, Portugal, 2017
  - 2nd edition, Roma, Italy, 2016
- 26.6. Chair dell'International Workshop on Emerging Technologies for Authorization and Authentication (ETAA), Co-Located with ESORICS
- 5th edition, Copenhagen, Denmark, 2022
  - 4th edition, online streaming, 2021
  - 3rd edition, online streaming, 2020
  - 2nd edition, Luxemburg, 2019
  - 1st edition, Barcellona, Spain, 2018
- 26.5. Chair del 2nd Distributed Ledger Technology Workshop (DLT 2019), Co-located with the Third Italian Conference on Cybersecurity (ITA-SEC 2019), Pisa, Italy, 2019
- 26.4. Co-chair della Special Session on Blockchain Technologies and Economics della 15th International Conference on Economics of Grids, Clouds, Systems & Services (GECON 2018), Pisa, Italy, 2018, <http://2018.gecon-conference.org>
- 26.3. Organizzatore del workshop TEchnical and LEgal aspects of data pRivacy and SEcurity, (TELERISE)
- 3rd edition, Trento, Italy, Affiliated with SAFECOMP 2017
  - 2nd edition, Lugano, Switzerland, Affiliated with ICWE 2016
  - 1st edition, Firenze, Italy, Affiliated with of ICSE 2015
- 26.2. Co-chair della Fourth International Symposium on Security in Collaboration Technologies and Systems (SECOTS 2014), part of The 2014 International Conference on Collaboration Technologies and Systems (CTS 2014)
- 26.1. Co-chair del Workshop on Dependability and Interoperability in Heterogeneous Clouds 2013 (DIHC 2013), workshop colocated with Europar 2013
- 27. Comitati di Programma di Conferenze e Workshop Internazionali**
- 27.71. TPC member del 41st ACM/SIGAPP Symposium On Applied Computing (SAC 2026)
- 27.70. TPC member del 7th Workshop on Blockchain theoRy and ApplicatIoNs 2026 (BRAIN 2026), hosted at the 24th IEEE International Conference on Pervasive Computing and Communications (PerCom 2026)
- 27.69. TPC member della Italian Conference on CyberSecurity 2025 (ITASEC25)
- 27.68. TPC member del 7th Distributed Ledger Technology Workshop (DLT 2025)
- 27.67. TPC member del 8th IEEE International Conference on Blockchain (IEEE Blockchain 2025)
- 27.66. TPC member del 6th Workshop on Blockchain theoRy and ApplicatIoNs 2025 (BRAIN 2025), hosted at the 23rd IEEE International Conference on Pervasive Computing and Communications (PerCom 2025)
- 27.65. TPC member del 7th IEEE International Conference on Blockchain (IEEE Blockchain 2024)
- 27.64. TPC member del 6th Distributed Ledger Technology Workshop (DLT 2024)
- 27.63. TPC member del 5th Workshop on Blockchain theoRy and ApplicatIoNs 2024 (BRAIN 2024), hosted at the 22nd IEEE International Conference on Pervasive Computing and Communications (PerCom 2024)
- 27.62. TPC member della IEEE International Conference on Blockchain and Cryptocurrency 2024 (IEEE ICBC'24)
- 27.61. TPC member della Italian Conference on CyberSecurity 2024 (ITASEC24)
- 27.60. TPC member del 1st Workshop on Theory of Smart Contracts and Applications (TOSCA2023), hosted at 25th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC 2023)
- 27.59. TPC member del 1st Workshop on Fintech and Decentralized Finance (FiDeFix23)

- 27.58.TPC member della Italian Conference on CyberSecurity 2023 (ITASEC23)
- 27.57.TPC member del 9th International Symposium on Security and Privacy in Social Networks and Big Data (SocialSec 2023)
- 27.56.TPC member del 4th Workshop on Blockchain theoRy and ApplicatIoNs 2023 (BRAIN 2023), hosted at the 21st IEEE International Conference on Pervasive Computing and Communications (PerCom 2023)
- 27.55.TPC member della IEEE International Conference on Blockchain and Cryptocurrency 2023 (IEEE ICBC'23)
- 27.54.TPC member del 4th Distributed Ledger Technology Workshop (DLT 2022), Co-located with ITASEC22
- 27.53.TPC member del Third Workshop on Blockchain Theory and Applications (BRAIN 2022) hosted at the 20th IEEE International Conference on Pervasive Computing and Communications (PerCom 2022)
- 27.52.TPC member della The 13th IEEE International Conference on Cloud Computing Technology and Science (IEEE CloudCom 2022)
- 27.51.TPC member della 19th International Conference on the Economics of Grids, Clouds, Systems, and Services (GECON2022)
- 27.50.TPC member del 9th Workshop on Large Scale Distributed Virtual Environments (LSDVE 2022) held in conjunction with ISCC 2022
- 27.49.TPC member della 23rd IEEE International Conference on High Performance Computing and Communications (IEEE HPCC-2021)
- 27.48.TPC member del 8th Workshop on Large Scale Distributed Virtual Environments (LSDVE 2021) held in conjunction with EURO-PAR 2021
- 27.47.TPC member del 2nd Workshop on Blockchain theoRy and ApplicatIoNs (BRAIN 2021) held in conjunction with ISCC 2021
- 27.46.TPC member della Italian Conference on CyberSecurity 2021 (ITASEC21)
- 27.45.TPC member del Trends in Distributed Ledger Technology Workshop (Trends in DLT 2021)
- 27.44.TPC member della 18th International Conference on the Economics of Grids, Clouds, Systems, and Services (GECON2021)
- 27.43.TPC member del 21th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID2021)
- 27.42.TPC member del The 2020 IEEE International Conference on High Performance Computing and Communications (IEEE HPCC-2020)
- 27.41.TPC member del 1st Workshop on Blockchain theoRy and ApplicatIoNS (BRAIN), Co-located with the 25th IEEE Symposium on Computers and Communications (ISCC 2020)
- 27.40.TPC member della 12th IEEE International Conference on Cloud Computing Technology and Science (IEEE CloudCom 2020)
- 27.39.TPC member della 17th International Conference on the Economics of Grids, Clouds, Systems, and Services (GECON2020)
- 27.38.TPC member della Italian Conference on CyberSecurity 2020 (ITASEC20)
- 27.37.TPC member del 3rd Distributed Ledger Technology Workshop (DLT 2020), Co-located with ITASEC20
- 27.36.TPC member del 2nd International Workshop on Future Perspective of Decentralized Applications (FPDAPP 2019) held in conjunction with the 25th International European Conference On Parallel And Distributed Computing (EUROPAR 2019)
- 27.35.TPC member del 16th International Conference on the Economics of Grids, Clouds, Systems, and Services (GECON 2019)
- 27.34.TPC member del 21st IEEE International Conference on High Performance Computing and Communications (HPCC-2019)
- 27.33.TPC member del 2019 IEEE International Conference on Communications (ICC): Communication and Information Systems Security Symposium (IEEE ICC'19 CISS)

- 27.32.TPC member del 18th IEEE International Conference on Computer and Information Technology (IEEE CIT 2018)
- 27.31.TPC member del 20th IEEE International Conference on High Performance Computing and Communications (HPCC 2018), Exeter, UK
- 27.30.TPC member del 13th International Conference on Availability, Reliability and Security (ARES 2018)
- 27.29.TPC member del Sixth Workshop on Large Scale Distributed Virtual Environments (LSDVE 2018)
- 27.28.TPC member del 10th IEEE International Conference on Cloud Computing Technology and Science (IEEE CloudCom 2018)
- 27.27.TPC member del ERCIM-Blockchain 2018 ERCIM Workshop on Blockchain Engineering: Challenges and Opportunities for Computer Science Research
- 27.26.TPC member del IEEE International Conference on Communication and Information Systems Security Symposium (IEEE ICC'18 CISS)
- 27.25.TPC member del 9th IEEE International Conference on Cloud Computing Technology and Science (CloudCom 2017)
- 27.24.TPC member del 13th IEEE International Conference on Green Computing and Communications (GreenCom-2017)
- 27.23.TPC member del IEEE ICC 2017 Communication and Information Systems Security Symposium (ICC'17 CISS)
- 27.22.TPC member del 17th IEEE International Conference on Computer and Information Technology (IEEE CIT 2017)
- 27.21.TPC member del 32nd International Conference on ICT Systems Security and Privacy Protection (IFIP SEC 2017)
- 27.20.TPC member del 2nd EAI International Conference on Smart Objects and Technologies for Social Good (GoodTech 2016)
- 27.19.TPC member del The 6th International Symposium on Security in Collaboration Technologies and Systems (SECOTS 2016), part of The 2016 International Conference on Collaboration Technologies and Systems (CTS 2016)
- 27.18.TPC member del The International Cross Domain Conference and Workshop (CD-ARES 2016)
- 27.17.TPC member del The Seventh International Conference on Cloud Computing, GRIDs, and Virtualization, 2016 (Cloud Computing 2016)
- 27.16.TPC member del The 9th EAI International Conference on Mobile Multimedia Communications (MOBIMEDIA 2016)
- 27.15.TPC member del The first domain specific Model-based Approach to Verification and validation (AMARETTO 2016)
- 27.14.TPC member del The 15th IEEE International Conference on Computer and Information Technology (CIT-2015)
- 27.13.TPC member del The 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TRUSTCOM 2015)
- 27.12.TPC member del Fifth International Symposium on Security in Collaboration Technologies and Systems (SECOTS 2015), part of The 2015 International Conference on Collaboration Technologies and Systems (CTS 2015)
- 27.11.TPC member del The Sixth International Conference on Cloud Computing, GRIDs, and Virtualization, 2015 (Cloud Computing 2015)
- 27.10.TPC member del 1st International Conference on Information Systems Security and Privacy (ICISSP 2015)
- 27.9.TPC member del Workshop on Dependability and Interoperability in Heterogeneous Clouds 2014 (DIHC 2014), workshop colocated with Europar 2014
- 27.8.TPC member del 6th International Symposium on Cyberpace Safety and Security (CSS 2014)
- 27.7.TPC member del The Fifth International Conference on Cloud Computing, GRIDs, and

- Virtualization, 2014 (Cloud Computing 2014)
- 27.6.TPC member della Security and Privacy track at the 5th IEEE International Conference on Cloud Computing Technology and Science 2013 (IEEE CloudCom 2013)
- 27.5.TPC member del Third International Symposium on Security in Collaboration Technologies and Systems (SECOTS 2013), part of The 2013 International Conference on Collaboration Technologies and Systems (CTS 2013)
- 27.4.TPC member del International Symposium on Security in Collaboration Technologies and Systems (SECOTS 2012), part of The 2012 International Conference on Collaboration Technologies and Systems (CTS 2012)
- 27.3.TPC member del International Symposium on Security in Collaboration Technologies and Systems (SECOTS 2011), part of The 2011 International Conference on Collaboration Technologies and Systems (CTS 2011)
- 27.2.TPC member del Context-Awareness Trust and Web 2.0 Trust 2009 (EuroCAT 2009)
- 27.1.TPC member del First International Workshop on Security, Trust and Privacy in Grid Systems (GRID-STP 2007), part of SecureComm 2007

Montelupo Fiorentino, 1 febbraio 2026

In fede,  
Paolo Mori  
firmato digitalmente



PAOLO MORI  
01/02/2026 12:33:17 UTC+0100